Tampereen yliopisto

Juha Savimäki

VERKKOKAUPAN TIETOTURVA

Diplomityö
Tekniikan ja luonnontieteiden tiedekunta
Matti Monnonen
Marko Helenius
09 / 2020

TIIVISTELMÄ

Juha Savimäki: Verkkokaupan tietoturva
Diplomityö
Tampereen yliopisto
Johtamisen ja tietotekniikan DI-ohjelma
09 / 2020

Tämän diplomityön aiheena on verkkokaupan tietoturva. Aiheen käsittely tehdään yleisellä tasolla rajautuen avoimen lähdekoodin ilmaisiin verkkokauppaohjelmistoihin. Diplomityön alussa esitellään teoriaa tietoturvasta ja eritoten verkkokauppoihin liittyvästä tietoturvasta, joihin kuuluvat verkkokauppaohjelmistojen lisäksi käyttäjät ja tietoliikenneverkot, sekä erilaiset laitteet ja niiden ohjelmistot.

Diplomityö pyrkii tuomaan esille verkkokauppaan liittyviä tietoturvariskejä ja tarjoamaan niihin toimivia, sekä tietoturvaa parantavia ratkaisuja. Käsitellyt tietoturvariskit vaikuttavat niin verkkokaupan toimintaan, kuin siellä vierailevien asiakkaiden turvallisuuteen. Samalla tutustutaan myös tietoturvariskejä hyödyntävien vihamielisten toimijoiden näkökulmaan.

Tässä diplomityössä käytetään perinteisen ohjelmistoprojektin vesiputousmallia, jossa todetaan jokaisen vaiheen tuovan omia huomioitaan verkkokaupan tietoturvan näkökulmasta. Diplomityö siis käsittelee, kuinka verkkokaupan määrittely ja suunnittelu tulee toteuttaa. Tämän jälkeen käsitellään verkkokaupan toteutusta verkkokaupan asennuksesta aina erilaisiin tietoturvaan vaikuttaviin konfiguraatioihin, sekä näiden lisäksi tarvittaviin verkkokauppaohjelmistoon liittymättömiin ylimääräisiin tietoturvaratkaisuihin.

Valmiin verkkokaupan toteutusvaiheen jälkeen seuraa testausvaihe. Testausvaihetta käsittelevässä kappaleessa tietoturvan kannalta olennaisimmat, sekä myös perinteisen ohjelmistoprojektin testausvaiheen käytännöt. Onnistuneen testaamisen jälkeen seuraa kappale ylläpitovaiheesta, jossa käsitellään verkkokaupan tietoturvallisena pitämistä erilaisin seurannan metodein ja päivittämällä verkkokauppaa säännöllisesti. Samalla tarkastellaan myös verkkokaupan tulevaisuuden näkymiä yleisellä tasolla ja mahdollisia skenaarioita verkkokaupan kehityksen suunnille.

Lopuksi vedetään vielä yhteen koko diplomityön sisältö yhteenvedossa, sekä pohditaan mahdollisia kohteita jatkotutkimusta varten. Myös diplomityössä käytetyn sisällön lähteet löytyvät diplomityön lopusta.

Avainsanat: Diplomityö, verkkokauppa, tietoturva, hakkerointi, suojaaminen, avoin lähdekoodi, open source, ohjelmistoprojekti, verkkokauppaohjelmisto, vesiputousmalli, tietoturvauhat, päätelaitteet, käyttäjät, tietoliikenneverkot, social engineering, palvelimet, ohjelmistot, vaatimusmäärittely, verkkokaupan rakentaminen, testaaminen, ohjeistaminen, korjaukset, testitapaukset, seuranta, ylläpito ja tulevaisuuden visiot.

ABSTRACT

Juha Savimäki: Ecommerce Security
Master's Thesis
Tampere University
Master's Programme in Management and Information Technology
09 / 2020

This Master's Thesis focuses on ecommerce security. The exact focus is on general level and mostly limited to free open source ecommerce platforms. In the beginning the masters thesis introduces theory of IT security, especially ecommerce security, which includes users, networks, hardware and software together with ecommerce platforms.

The Master's Thesis brings up security risks on ecommerce and gives functional solutions for those to improve ecommerce security. These security risks cover ecommerce platform functionalities as well as customer security. It also covers briefly the security risk exploits from hostile actors point of view.

This Master's Thesis uses traditional software project waterfall model, where it is noted that each step of the model brings something relevant to the ecommerce security. For starters, this means it covers how ecommerce requirements and design should be implemented. After that, it covers implementation of the ecommerce platform from installation to configurations and also some additional solutions to protect the online store.

After the implementation phase, there is a testing phase. Testing phase chapter covers the most relevant security topics together with testing procedures in a traditional software project. Next follows a maintenance phase chapter, where the focus is keeping the ecommerce platform, meaning the online store secure and up to date using different monitoring methods and regular software updates. Also future visions are covered in general level with possible scenarios of ecommerce development.

Finally, the whole Master's Thesis is wrapped up in a conclusion part, which also includes speculation of potential areas for further analysis. In the end there is a list of source material.

Keywords: Master's Thesis, ecommerce, online store, online shop, security, hacking, protection, open source, software project, ecommerce platform, waterfall model, security risks, hardware, users, networks, social engineering, servers, software, requirements, implementation, testing, instructions, fixes, test cases, monitoring, maintenance and future visions.

ALKUSANAT

Tämä diplomityö on tehty oman mielenkiinnon ja työkokemuksen pohjalta valitusta aiheesta, joka mielestäni on jatkuvasti ajankohtainen ja vaatisi julkisuudessakin ahkerampaa seurantaa. Suomessa tietoturva ei välttämättä saa täysin ansaitsemaansa huomiota ja toivottavasti tämä diplomityö auttaa osaltaan verkkokauppaan liittyvän tietoturvan kehitystä. Kiitokset läheisille tuesta ja maltista kirjoittamisen ajalta, sekä ohjaajalle avusta!

Vantaalla, 3.9.2020

Juha Savimäki

SISÄLLYSLUETTELO

KUVALUETTELO

LYHENTEET JA MERKINNÄT

chmod	Change mode, tiedostojen ja hakemistojen käyttäjäoikeuksien hallinta
GDPR	General Data Protection Regulation, yleinen tietoturva-asetus
HTTP	Hypertext Transfer Protocol, protokolla
HTTPS	Hypertext Transfer Protocol Secure, suojausprotokolla
ICT	Information and communication technology, tieto- ja viestintätekniikka
IP	Internet Protocol, verkkoprotokolla
LDAP	Lightweight Directory Access Protocol, verkkoprotokolla
NSA	National Security Agency, Yhdysvaltain kansallinen turvallisuusvirasto
OWASP	Open Web Application Security Project, verkkoturvallisuusprojekti
PHP	PHP: Hypertext Preprocessor, ohjelmointikieli
SQL	Structured Query Language, ohjelmointikieli
TLS	Transport Layer Security, salausprotokolla
URL	Uniform Resource Locator, verkko-osoite
WWW	World Wide Web, hypertekstijärjestelmä

.

1. JOHDANTO

Tämän diplomityön aiheena on verkkokaupan tietoturva ja se pyrkii nostamaan esille kuinka paljon erilaisia tietoturvaan liittyviä asioita verkkokaupan perustaminen ja ylläpitäminen sisältävät. Usein puhutaan yleisellä tasolla siitä, että Suomessa ollaan jäljessä tietoturvan osaamisessa ja siihen panostamisessa. Tämä käy käytännössä ilmi esimerkiksi juuri yksittäisten pienten toimijoiden verkkokaupoista, jossa kauppa on perustettu ilman sen suurempaa osaamista asiasta. Näissä tilanteissa niin kauppias, kuin asiakaskin altistuvat erilaisille verkon tuomille uhille.

Tässä diplomityössä tuodaan esille erilaisia näkökulmia verkkokauppaan liittyvistä uhista, kuten verkkokaupan ohjelmistoon ja sen konfigurointiin liittyvät uhat, sekä näiden lisäksi tietoliikenneverkkoihin, palvelimiin, päätelaitteisiin, laitteiden ohjelmistoihin ja käyttäjiin liittyviä tietoturvauhkia.

Seuraavassa, eli toisessa luvussa, käydään läpi verkkokaupan tietoturvan teoriaa. Siinä esitellään yleisimpiä asioita ja keinoja, joita on otettava huomioon verkkokaupassa tai verkkosivustoprojekteissa yleisesti. Näitä asioita on käsitelty edellisessä kappaleessa mainituista näkökulmista.

Kolmannessa luvussa keskitytään suojatun verkkokaupan rakentamiseen. Siinä esitellään aluksi yleisimpiä tietoturvariskejä ja niiden lisäksi ohjelmistoprojektin vesiputousmalli. Tämän vesiputousmallin pohjalta ensimmäisenä vaiheena esitellään vaatimusmäärittely, jossa avataan verkkokauppaan tarvittavien ominaisuuksien, eli vaatimusten dokumentointia. Tämä jälkeen siirrytään valitsemaan laitteita ja ohjelmistoja, sekä tehdään tarvittavat asennustoimenpiteet ja konfiguroinnit. Tässä luvussa esitellään myös testaamisen valmisteluja ja käyttäjien ohjeistamista.

Neljäs luku käsittelee verkkokaupan tietoturvan testaamista ja sen pohjalta tehtäviä korjauksia. Siinä luvussa keskitytään aluksi verkkokaupan ohjelmistoihin, sekä laitteisiin ja niiden omiin ohjelmistoihin. Sen jälkeen käsittelyssä on tietoliikenneverkkojen testaaminen ja kuinka käyttäjät tulee huomioida testausprosessissa. Lopuksi tarkastellaan verkkokaupan tarvittavia korjaustoimenpiteitä, joiden tarve on havaittu testauksen pohjalta.

Viidennessä luvussa tarkastellaan verkkokaupan ylläpitoa ja seurantaa. Siinä käsitellään ensimmäisenä verkkokaupan seurannan mahdollisuuksia ja siihen kohdistuvia ulkopuo-

listen tahojen asettamia rajoituksia. Tämän jälkeen käydään läpi ylläpitoon kuuluvat päivitykset ja muut ylläpidolliset tehtävät. Lopussa analysoidaan verkkokaupan tulevaisuudennäkymiä kolmen pääperiaatteen pohjalta ja esitetään näkemyksiä mahdollisista verkkokaupan suuntauksista.

Kuudennessa luvussa diplomityö vedetään yhteen tarkastelemalla tiivistetysti edellisissä luvuissa käsiteltyjä asioita ja pohdiskelemalla niistä kumpuavia ajatuksia, sekä mahdollisia jatkotutkimusaiheita.

Tämän diplomityön tuloksena saadaan kokonaisvaltainen näkemys verkkokaupan tietoturvaan liittyvistä osa-alueista, huomioista ja tarvittavista toimenpiteistä.

2. VERKKOKAUPAN TIETOTURVAN TEORIAA

Tässä luvussa käsitellään verkkokaupan tietoturvan kannalta keskeisimpiä uhkia teoriatasolla. Näihin kuuluvat verkkokauppaohjelmistoihin suoraan kohdistuvien tietoturvauhkien lisäksi laitteisiin ja niiden ohjelmistoihin kuuluvat uhat, kuin myös tietoliikenneverkkojen, vihamielisten toimijoiden ja käyttäjien itsensä omalla toiminnallaan aiheuttamat uhat. Diplomityön laajuuden asettamien rajojen vuoksi tarkastelusta jätetään pois yksityiskohtaisemmat tekniset käsittelyt.

Yleisesti on todettava, ettei verkkokaupan tietoturvaa saa asetettua kerralla kuntoon, vaan tietoturva vaatii jatkuvaa ylläpitämistä. Käytännössä tämä tarkoittaa sitä, että kun tässä diplomityössä käsitellyt vaiheet on suoritettu, pitäisi prosessi aloittaa joiltain osin uudestaan päivittämällä ohjelmistoa, laitteistoa ja muita osa-alueita. Verkkokauppaa on myös jatkuvasti tarkkailtava epäilyttävän toiminnan havaitsemiseksi ja sen torjumiseksi riittävän tehokkain keinoin.

Euroopan Unionissa tietoturvaa säädellään henkilötietojen ja niihin liittyvien arkaluonteisten tietojen osalta yleisellä tietoturva-asetuksella, josta käytetään lyhennettä GDPR (engl. General Data Protection Regulation). Tämän asetuksen myötä myös verkkokauppojen on täytettävä sen vaatimat ehdot ja tarjottava asiakkailleen mahdollisuutta nähdä tai muokata omia henkilötietojaan tietoturva-asetuksen edellyttämällä tavalla. Tässä diplomityössä GDPR-asetus esitellään näin yleisellä tasolla, sillä se liittyy olennaisena osana verkkokaupan suunnitteluun, mutta sen vaatimien toimenpiteiden tarkempi käsittely ei tuo lisäarvoa diplomityön kokonaisuuteen. Tietosuoja-asetus sisältää kuitenkin teknisiä ja organisatorisia ehtoja, joiden oletetaan myöhemmissä luvuissa täyttyvän verkkokaupan osalta. [24] Myös muilla julkisilla toimijoilla saattaa olla omia rajoituksiaan tietoturvaan, tietojen käsittelyyn, myyntikäytäntöihin, markkinointiin tai tuotteisiin liittyen, mutta nekin rajataan pois tämän diplomityön aihepiiristä.

Verkkokaupan tietoturvaan liittyy olennaisena osana vihamieliset hyökkäykset verkkokauppaa tai siihen olennaisesti liittyvää osa-aluetta vastaan, jolloin on myös tärkeää osata reagoida näihin oikein ja kyetä torjumaan hyökkäykset. Hyvänä käytäntönä on raportoida yksityiskohtaisesti kaikki havaitut hyökkäykset poliisille ja tarpeen mukaan myös ohjelmiston tai laitteen valmistajalle ja muille asianosaisille, kuten käyttäjille. Joskus tätä raportointia myös vaaditaan tietoturvaa loukkaavissa tilanteissa.

Tässä diplomityössä käsitellään myös käyttäjän näkökulmaa, varsinkin asiakkaan kannalta, koska asiakkaiden luottamus verkkokauppaa kohtaan on avainasemassa verkkokaupan menestymisen kannalta. Verkkokaupassa liikkuu paljon erilaisia asiakastietoja ja niitä tallennetaan yleensä useisiin tietokantoihin, jolloin näissä tiedoissa ja tietokannoissa saattaa olla myös paljon erilaisia arkaluonteisia yksityiskohtia. Uutiset ja puheet vuodetuista asiakastiedoista tai tietoturvaongelmista leviävät helposti eteenpäin ja saattavat aiheuttaa lopun kyseisen verkkokaupan toiminnalle, sekä aiheuttaa verkkokaupan asiakkaille pitkäkestoisia murheita. Erityisen haitallisia verkkokaupan asiakkaille on henkilötunnusten vuotaminen. Henkilötunnuksia käytetään verkkokaupoissa laskulla maksamisen ja osamaksun mahdollistamiseksi. Suomessa on tapahtunut erilaisia tietovuotoja, joissa väärin perustein haltuun saaduilla henkilötunnuksilla on tilattu erilaisia asioita uhrin laskuun. Näin on käynyt esimerkiksi Työtehoseuran ja Itä-Suomen yliopiston järjestelmistä vuotaneille tiedoille, jossa 16000 suomalaisen nimet, osoitteet, puhelinnumerot ja henkilötunnukset pääsivät vuotamaan vihamielisille toimijoille. Tämän tietovuodon pohjalta on uhrien henkilötunnuksia hyödyntäen tapahtunut tuhansia rikoksia vuosittain. [6]

2.1 Verkkokauppaohjelmistot

Verkkokauppaohjelmisto on verkkokaupan toiminnan kannalta ydinasemassa ja usein verkkokauppoja vastaan tehtävät vihamieliset hyökkäykset kohdistuvat juuri itse verkkokauppaohjelmistoon, jolloin se on myös tietoturvan näkökulmasta keskeisimpiä asioita verkkokaupassa. Toisaalta verkkokauppaohjelmisto saattaa myös virhetilanteessa paljastaa erilaisia salatuiksi tarkoitettuja asioita, jolloin hyökkäysten torjunta ei ole ainoa tietoturvan tason määrittävä tekijä. Näitä käsitellään tarkemmin myöhemmässä vaiheessa, mutta ensin tarkastellaan erilaisia ohjelmistoja.

Erilaisia verkkokauppaohjelmistoja on olemassa lukuisia ja niitä voidaan luokitella erilaisten kriteerien pohjalta, kuten toteutuksen tai palvelukokonaisuuden perusteella. Näillä tarkoitetaan käytännössä sitä, millä ohjelmointi- ja määrittelykielillä verkkokauppa on toteutettu tai onko ohjelmisto pelkkä asennettava paketti vai tarjotaanko se valmiina avaimet käteen -pakettina ylläpidetyllä palvelimella käyttömaksua vastaan.

Tässä diplomityössä tullaan keskittymään enimmäkseen ilmaisiin avoimen lähdekoodin verkkokauppaohjelmistoihin, kuten OpenCart -verkkokauppaohjelmistoon, ja rajataan muut ratkaisuvaihtoehdot käsittelyn ulkopuolelle. Tämä valinta on tehty siksi, että ilmai-

set avoimen lähdekoodin verkkokauppaohjelmistot voivat perehtymättömän verkkokaupan perustajan toimesta aiheuttaa paljon riskitekijöitä tietoturvan kannalta, jolloin se soveltuu hyvin käsiteltäväksi tämän diplomityön aihepiiriin. Seuraava Taulukko 1 havainnollistaa verkkokauppaohjelmistojen valinnanvaraa pelkästään ilmaisuuden ja avoimen lähdekoodin pohjalta, listaamalla ecommerce-platforms.com -verkkosivuston mukaan 20 suosituinta verkkokauppaohjelmistoa tästä kategoriasta [22].

Taulukko 1. *Suosituimmat ilmaiset avoimen lähdekoodin verkkokauppaohjelmistot [22].*

Sijoitus	Verkkokauppaohjelmisto	Sijoitus	Verkkokauppaohjelmisto
1	Square Online Store	11	JigoShop
2	WooCommerce	12	Drupal Commerce
3	CS-Cart Multi-Vendor	13	WP eCommerce
4	nopCommerce	14	Ubercart
5	X-Cart	15	Wix Ecommerce
6	Zen Cart	16	Branchbob
7	Magento Open Source	17	Big Cartel
8	OpenCart	18	Jimdo
9	PrestaShop	19	Ecwid
10	osCommerce	20	Weebly

Tämä Taulukko 1 sisältää samasta kategoriasta puhtaasti itsenäisenä verkkokauppana toimivat verkkokauppaohjelmistot, kuten OpenCart, ja tietyn sisällönhallintajärjestelmän päällä toimivat verkkokauppaohjelmistot, kuten WooCommerce, joka toimii WordPress-sisällönhallintajärjestelmän päällä.

Kun tarkastellaan tätä eroavaisuutta itsenäisen verkkokaupan ja sisällönhallinnan päälle rakennetun välillä voidaan havaita, ettei selkeää tutkimukseen pohjaavaa faktapohjaista eroa löydy tietoturvan kannalta. Voidaan ajatella, että yhden ohjelmiston tietoturvaa on helpompaa hallita, mutta toisaalta sisällönhallinnan päälle rakennetulla kaupalla saattaa olla etuja ainakin päivityksien suhteen, jos myöskin enemmän paikattavia tietoturva-aukkoja. Toisaalta myös verkkokauppaohjelmiston tai sisällönhallintajärjestelmän suosio vaikuttaa tietoturvaan, sillä suuremman suosion keräävät ohjelmistot ja järjestelmät herättävät myös suurempaa kiinnostusta vihamielisten toimijoiden keskuudessa.

Suosioon ja tietoturvan ongelmiin liittyen on pitkään uutisoitu WordPressin ja sen lisäosiin liittyvistä tietoturvauhista. ICT-alan (engl. Information and communication technology) erikoisjulkaisu Tivin mukaan WordPress on maailman suosituin sisällönhallintajärjestelmä ja siitä huolimatta se on alun perin kehitetty blogien kirjoittamista varten. WordPress -sisällönhallintajärjestelmään on vain ajan saatossa kehitetty lukuisia erilaisia lisäosia erilaisiin käyttötarkoituksiin. Näin ollen suosio, sekä lisäosien ja varsinaisen WordPressin tietoturvaongelmat tekevät siitä hyvin houkuttelevan kohteen hyökkääjille. Kun nämä vihamieliset hyökkääjät löytävät yhden tietoturva-aukon WordPressistä tai siitä ja sen lisäosien yhdistelmistä, niin he pääsevät hyödyntämään sitä lukuisiin sivustoihin, jossa kyseinen WordPress-versio tai yhdistelmä on käytössä. Tivi listaa tästä esimerkin keväältä 2020, jossa varoitetaan verkkokauppoja seuraavan lisäosan käytöstä: Flexible Checkout Fields for WooCommerce. [9]

Wordpressin suosion etuna on tietysti tiheä päivitystahti, jolla pyritään paikkaamaan sisällönhallintajärjestelmään itseensä jääneet tietoturvaongelmat. Tosin WordPressiä käyttämällä verkkokauppaa varten tarvitaan lisäosia ja näillä on jokaisella omat päivitysaikataulunsa, jolloin suojauksesta ei pelkän päivityksen keinoin saada vielä riittävän kattavaa.

Itsenäisellä verkkokauppaohjelmistolla päivitystahti ei välttämättä myöskään ole ripeää. Tästä käy hyvänä esimerkkinä OpenCart, jolla nykyisen version 3.0.3.3 ja edellisen version 3.0.3.2 julkaisupäivien välillä on yli vuosi, eikä tästä huolimatta päivityksissä ole välttämättä tietoturvaan liittyviä korjauksia. [15] Toisaalta myös OpenCartiin on saatavilla paljon lisäosia, varsinkin maksu- ja toimitustapoja varten, jolloin näiden tietoturva ja päivitystahti aiheuttavat omat riskinsä verkkokaupan toiminnalle. Yksittäisiä ohjelmistoihin ja niiden lisäosiin liittyviä riskejä on lukemattomia, joten ne on rajattava ulos tästä diplomityöstä ja keskityttävä joihinkin yleisimpiin tietoturvauhkiin.

Verkkokauppaohjelmistoissa voi olla virheistä johtuvia tai myös sen ominaisuuksiin kuuluvia tiedonpalasia näkyvillä eri puolilla verkkokauppaa, jolloin vihamielinen toimija voi kerätä tarvitsemansa tiedot näistä pienistä palasista verkkokaupan eri sivuilta ja osioista. Näitä tietoja voivat esimerkiksi olla hakemistorakenteet, tiedostonimet ja tiedostolistaukset, mutta myös versionumerot, liian kuvaavat virheilmoitukset tai muut arkaluonteiset tiedot itse verkkokaupasta.

Monissa verkkokaupoissa on käytössä jonkinlainen lomake, jonka avulla asiakas tai verkkokaupan henkilöstö saa lähetettyä vapaamuotoista tai jollain tavalla rajoitettua tekstiä, joka voi sisältää myös koodia. Näitä lomakkeita voi myös olla pelkkä sisäänkirjautumislomake verkkokauppaan. Yksinkertaisimmissa verkkokaupan toteutuksissa voi

sisäänkirjautumisen tapauksessa onnistua hyökkääminen LDAP-injektion (engl. Lightweight Directory Access Protocol) avulla, jolloin syötteeseen annetaan tarvittavia lisämerkkejä. Myös evästetietoja muokkaamalla saadaan vaikutettua sisäänkirjautumiseen ja erilaisiin sessioihin. Suuremmissa lomakkeissa yleisimpinä tapoina käytetään SQL-injektiota (engl. Structured Query Language) tai muita koodiin ja tietokantaan liittyviä muokkauksia. [21, s. 234-246]

Verkkokauppaohjelmistot tarjoavat verkkokauppahenkilöstölle mahdollisuutta lähettää sähköpostia verkkokaupan asiakkaille, joko automaattisesti tai manuaalisesti. Nämä sähköpostit liittyvät verkkokaupassa asiointiin, kuten tilaamiseen ja toimituksen tilamuutoksiin, jolloin verkkokauppaohjelmistosta lähtee sähköpostitse automaattinen kuittaus vastaanottajalle. Manuaalisesti viestejä lähetetään käytännössä kohdennetulle yksittäiselle asiakkaalle poikkeavissa tilanteissa, kuten toimitusongelmissa. Verkkokauppaohjelmiston lähettämiin ja myös sitä kautta lähetettäviin manuaalisiin sähköposteihin liittyy tietoturvariskejä. Pääsääntöisesti nämä muodostuvat oletusarvoisten lähetystietojen, sekä sähköpostipohjien käyttämisestä, jolloin vastaanottaja voi mahdollisesti nähdä sähköpostista lähettäjän käyttäjätunnuksen, yksityiskohtaisia tietoja palvelimesta tai verkkokaupan rakenteeseen liittyviä olennaisia tietoja. Vaikka vastaanottaja ei olisikaan vihamielinen taho, niin tämän käyttämä laitteisto voi olla altistunut vihamieliselle toimijalle tai sähköpostiliikenne voi vuotaa avoimesta verkosta, jolloin vastaanottaja tahtomattaan altistaa verkkokaupan mahdolliselle hyökkäykselle.

Jos vihamielinen toimija on valinnut tietyn kohteen, eikä siinä ole itsestään selviä näkyviä tietoturva-aukkoja, tämä vihamielinen toimija voi ottaa käyttöön niin sanotun footprinting-metodin, eli verkkokaupan sivuston tarkemman tutkinnan, jonka avulla verkkokaupasta hankitaan olennaista tietoa. Tämä voi tapahtua esimerkiksi peilaamalla koko verkkokaupan, eli kopioimalla sen lokaaliin ympäristöön, jolloin sen parissa tehtävä tutkimus voidaan tehdä herättämättä verkkokaupan ylläpidon huomiota. Tällä tutkimisella pyritään löytämään verkkokaupan olennaiset heikot kohdat tutustumalla verkkokaupan rakenteeseen. [21, s. 55-56]

2.2 Palvelimet

Palvelimien tietoturva rakentuu monesta eri osasta, mutta palvelimen fyysinen sijainti, verkkoratkaisut ja ohjelmisto vaikuttavat siihen olennaisimmin. Fyysisen sijainnin osalta palvelimen maantieteellinen sijainti ja palvelimen tai palvelinkeskuksen muu toiminta vai-

kuttaa vihamielisten toimijoiden hyökkäysyrityksiin. Erityisesti jos palvelimella tai samassa palvelinkeskuksessa sijaitsee suuryritysten tai valtiollisten tahojen tietoja tai toimintoja. Tällöin samassa fyysisessä sijainnissa toimiva verkkokauppa tai sen sisältö saattaa päätyä poliittisen tai rahanansainnan intressien sivutuotteena vihamielisen toimijan haltuun.

Hyökkäyksiä palvelimia kohtaan voidaan tehdä monella tapaa. Siksi onkin hyvä lähteä liikkeelle fyysisestä sijainnista ja eritoten tilasta, jossa palvelin sijaitsee. Tilan tulisi täyttää olennaiset tekniset vaatimukset ilmanvaihdosta ja varmistetusta sähkönjakelusta, sekä pääsy tiloihin tulisi rajata kulkuoikeuksin vain ja ainoastaan palvelimen ylläpidon kannalta tarpeellisille henkilöille. Myös verkkoyhteyksien liitännät ja kaapelointi tulisi olla toteutettuna niin, että fyysisten muutosten tekeminen olisi lähes mahdotonta. Tietoliikenneverkkoihin otetaan tarkemmin kantaa kohdassa 2.4, mutta ne on syytä mainita myös tässä palvelinten yhteydessä.

Verkkokaupan palvelimet sijaitsevat verkkoteknisesti palvelun luonteen vuoksi käytännössä aina julkisesti näkyvillä verkossa, jolloin ne näkyvät käytännössä kenelle tahansa ympäri maailman. Joissain tapauksissa verkkokauppa saattaa olla rajattuna myös verkossa maantieteellisen sijaintinsa mukaan tai tietyn tahon sisäisiin tarkoituksiin, mutta niitä rajoituksia ei käsitellä tässä diplomityössä sen tarkemmin.

Tämä palvelimen maailmanlaajuinen näkyvyys aiheuttaa sen, että vihamielinen toimija näkee palvelimen tai palvelinkeskuksen verkkolaitteet mistä tahansa. Tällöin palvelin on suojauksistaan huolimatta alttiina seurannalle tai hyökkäykselle. Seuranta ja hyökkäykset palvelimeen voivat tapahtua siis fyysisen vaihtoehdon lisäksi tietoliikenneverkon kautta ja erilaisia palvelinohjelmistojen haavoittuvuuksia hyödyntäen tai ohjelmoidun verkkokaupan kautta.

Ajoittain palvelimella ylläpidetään vanhoja päivittämättömiä verkkokauppoja, jotka käyttävät vanhentuneita versiota ohjelmista tai ohjelmointikielistä, kuten PHP-kielestä (engl. PHP: Hypertext Preprocessor). Itse PHP-kieltä päivitetään usein, mutta monesti vanhoissa verkkokauppaohjelmistoissa tuki ei riitä PHP:n uusimpiin versioihin ja tällöin palvelimelle jää vanha versio, joka yhdessä verkkokauppaohjelmiston kanssa aiheuttaa tietoturvariskin koko palvelimelle.

Yksi verkkokaupan tietoturvan kannalta tärkeä kohde, tietokanta, houkuttelee palvelimelle vihamielisiä toimijoita. Tietokanta, tai verkkokauppaohjelmistojen yhteydessä monesti useampi tietokanta, toimivat tiedon tallentamisessa kaupan toimintoja varten. Näihin tallennetaan tuotetietojen lisäksi tilaustietoja, eli asiakkaiden arkaluonteisia tietoja

henkilötiedoista maksutietoihin. Nämä tiedot ovat yksi suuri syy, miksi tietokantoja ja palvelimia vastaan tehdään hyökkäyksiä.

Nykyaikana verkkokaupat sijaitsevat hyvin usein pilvipalveluissa, jolloin tietoturva-asioista tulee moniulotteisempia, eivätkä perinteiset yksittäiseen palvelimeen kohdistuvat tietoturvametodit välttämättä päde. Tämän vuoksi tässä diplomityössä keskitytään perinteisiin palvelimiin ja palvelinkeskuksiin, joten rajataan pilvipalvelut diplomityön ulkopuolelle. Alla oleva Kuva 1 havainnollistaa verkkoon kytkettyjen erilaisten laitteiden yhteyttä toisiinsa.

Kuva 1. *Verkkokaavio [3].*

Kuva 1 siis esittää, kuinka pilven kautta puhelimet, tabletit, tietokoneet, tietokannat ja viihdelaitteet nivoutuvat yhteen samassa verkossa. Tämä tarkoittaa sitä, että pilvessä olevan datan avulla laitteet voivat kommunikoida keskenään tai jakaa sisältöä toisilleen tuntematta välttämättä tätä toista laitetta sen tarkemmin.

2.3 Päätelaitteet ja niiden ohjelmistot

Tässä yhteydessä päätelaitteilla tarkoitetaan käytännössä verkkokaupan ylläpidon ja käyttäjien laitteistoa, sekä rajataan ulos muut mahdolliset päätelaitteet, kuten palvelimen ylläpidon laitteistot. Näitä laitteita ovat esimerkiksi tietokoneet, tabletit, matkapuhelimet ja verkkolaitteet.

Käyttäjien ja ylläpidon päätelaitteille tunkeutuminen voi olla vihamieliselle toimijalle houkutteleva vaihtoehto hyvin suojatulle palvelimelle tai verkkokauppaan hyökkäämisen sijaan. Tämä voisi tapahtua käytännössä silloin, kun vihamielisellä toimijalla on tarkoitus hyötyä verkkokaupasta jollain tavalla, eikä vain haitata ja hidastaa sen toimintaa. Yleensä käyttäjät, sisältäen verkkokaupan ylläpitäjät, ovat tietoturvayhtälön heikoimpia lenkkejä. Sen vuoksi myös heidän päätelaitteensa ovat yksi varteenotettava etenemisväylä vihamieliselle toimijalle. Käyttäjät tekevät laitteillaan huomaamattaan tai vahingossa virheitä, kuten liittyvät suojaamattomiin langattomiin verkkoihin, klikkaavat auki viesteissä lähetettyjä linkkejä ja liitteitä, vierailevat epämääräisillä verkkosivuilla, käyttävät arvattavissa olevia salasanoja ja muuta vastaavaa. Toisaalta myös ohjelmistoissa on tietoturva-aukkoja, jolloin varsinkin päivittämättömät päätelaitteet ovat vaarassa ilman käyttäjän virhetoimintaa.

On olemassa myös monia esimerkkejä, joissa valtiolliset toimivat ovat olleet tietoisia tai tarkoituksella vaikuttaneet ohjelmistokehitykseen, jolloin päätelaitteiden käyttöjärjestelmiin tai ohjelmistoihin on saatu takaportteja tiedonkeruuta tai hyökkäystä varten. Näin on esimerkiksi käynyt Windows-käyttöjärjestelmillä varustetuille päätelaitteille Iranin ydinvoimaloihin liittyneessä tapauksessa. [5] Toisaalta Yhdysvaltalainen NSA (engl. National Security Agency), on ollut omalta osaltaan mukana kehittämässä Linux- ja Android-käyttöjärjestelmiä, jolloin heillä on ollut mahdollisuus rakentaa järjestelmiin haluttuja ominaisuuksia, ottamatta kantaa siihen ovatko he näin tehneet [12]. Myös sosiaalisen median profiilit ja applikaatiot on liitetty vastaavaan toimintaan, kuten esimerkiksi Kiinan valtion kytkökset suosittuun TikTok-palveluun [23]. Tällaiset mahdolliset ratkaisut kuitenkin harvoin kohdistuvat verkkokauppoihin ja yksittäisiin kaupallisiin toimijoihin, vaan enimmäkseen valtiollisiin kohteisiin tai yksittäisiin seurattaviin henkilöihin, joten ne rajataan pois tämän diplomityön aihepiiristä.

2.4 Tietoliikenneverkot

Tietoliikenneverkoissa on huomioitava niin verkkokaupan toimintaan liittyvät verkot, kuin myös verkkokaupan ylläpidon ja käyttäjän hyödyntämät verkkoratkaisut. Verkkokaupan toimintaan liittyvät verkot ovat pääsääntöisesti yllä olevaan palvelinta käsittelevään alalukuun kuuluvia, mutta niihin voi myös kuulua ulkoisien palveluiden palvelinten verkkoyhteydet, kuten verkkokaupan tapauksessa monesti maksupalveluihin liittyvät ratkaisut. Yksinkertaisuuden vuoksi, jätetään nämä kuitenkin pois tarkastelusta tämän diplomityön osalta.

Monesti ongelmatilanteet sattuvat päätelaitteen käytön yhteydessä tai johtuvat käyttäjän toiminnasta verkossa. Toimistojen verkoissa on oletusarvoisesti riittävä suojaus palomuurin ja kulunvalvonnan avulla, mutta kotitoimistolla tilanne voi usein olla täysin erilainen. Kotiverkon suojaaminen on monesti asukkaan itsensä varassa ja toisinaan kotiyhteyksinä käytetään siltaavia yhteyksiä, jolloin laitteet ovat suoraan näkyvissä ulkoverkkoon. Varsinaisissa toimistoissa ja palvelinkeskuksissa on huolehdittu riittävästä turvasta erinäisin laittein ja ohjelmistoin, kuten esimerkiksi oikein konfiguroidun palomuurin avulla.

Myös langattoman verkon käyttäminen muodostaa tietoturvan kannalta haasteita. Näissä riski on suurin avoimissa verkoissa, joihin kuka tahansa voi liittyä ja toimia niissä vapaasti. Näitä verkkoja löytyy niin kotoa, kuin kahviloista, julkisesta liikenteestä ja ylipäänsä julkisilta paikoilta. Verkkokauppojen näkökulmasta avointen verkkojen käyttäminen on erittäin huolestuttavaa varsinkin ylläpitäjien osalta, sillä verkkokaupan tunnukset ja asiakastiedot ovat tällöin vaarassa vuotaa vääriin käsiin avoimen verkon kautta.

Verkkokaupan kohdalla verkkojen tietoliikenne on myös syytä salata, ettei se olisi vapaasti luettavissa selkokielellä julkisessa verkossa. Käytettävän verkkokauppaohjelmiston on myös tuettava valittua suojausta. Suojaukseen käytetään erillistä salausprotokollaa, eli TLS-protokollaa (engl. Transport Layer Security), joka suojaa sovellusten tietoliikenteen IP-verkoissa (engl. Internet Protocol). Verkkokauppaohjelmistojen kohdalla TLS-protokollan yleisin käyttötapa on WWW-sivujen (engl. World Wide Web) siirron suojaaminen käyttäen HTTPS-protokollaa (engl. Hypertext Transfer Protocol Secure). Tämä HTTPS-protokolla rakentuu HTTP-protokollasta (engl. Hypertext Transfer Protocol) ja edellä mainitusta TLS-protokollasta. [17][21 s. 362-366] Tämän toteuttamiseen käytetään suojaussertifikaattia, joka voi olla kansainvälisesti tunnetun tahon myöntämä maksullinen sertifikaatti tai ilmainen sertifikaatti, jonka palveluntarjoaja on omista järjestelmistään luonut. Ilmainen sertifikaatti voi myös olla omatekoinen, jolloin jotkut Internet-selaimet huomauttavat siitä, kun tällä sertifikaatilla suojatulle verkkosivulle ollaan menossa. Vaikka omatekoiset sertifikaatit ovat periaatteessa yhtä turvallisia, kuin tunnettujen tahojen luomat, voi sertifikaatin tekijä kuitenkin hyödyntää luomaansa sertifikaattia vihamielisen sivun ylläpitämiseen ja tämän vuoksi selaimissa saattaa näkyä varoitus.

2.5 Social engineering ja käyttäjän toiminta

Social engineering, eli käyttäjän manipulointi, tarkoittaa sen kohteena olevan käyttäjän eri tavoilla toteutettua psykologista huijaamista vihamielisessä tarkoituksessa. Kuten aiemmin mainittiin, tietoturvassa yleensä käyttäjä on heikoin lenkki, varsinkin korkean

tietoturvatason omaavissa ratkaisuissa. Tällöin käyttäjän huijaaminen on helpoin ja nopein tapa päästä kiinni kohdejärjestelmään vihamielisessä tarkoituksessa.

Monesti suoraviivaisimmat ja yksinkertaisimmat tavat ovat tehokkaimpia käyttäjän manipuloinnissa, sillä käyttäjä ei ole valmistautunut niihin, eikä välttämättä osaa odottaa niitä tapahtuviksi. Usein ICT-alan esityksissä käytetäänkin esimerkkeinä tapauksia, joissa käyttäjän tunnukset on hankittu vääriin käsiin kysymällä niitä käyttäjältä itseltään. Näissä tilanteissa käyttäjään on vedottu erilaisilla psykologisilla tavoilla, jotka herättävät käyttäjässä luottamusta tai hämmentävät riittävästi, jotta tämä antaisi tunnuksensa vieraille. Käytännön esimerkkinä voisi kuvata keksityn tapauksen, jossa teknisenä tukena esiintyvä henkilö on onnistunut tunkeutumaan toimistoon ja tulee käyttäjän työpisteelle työskentelemään, kuin olisi tulossa korjaamaan ongelmaa. Muut ihmiset toimistossa näkevät tämän henkilön ja jos tämä henkilö onnistuu olemaan riittävän vakuuttava, käyttäjälle voi herätä vaarallinen luottamuksen tunne kyseiseen henkilöön. Jos käyttäjä on kuitenkin sen verran valppaana, ettei kysyttäessä anna tunnuksiaan, voi riskinä olla, että tämä vihamielinen henkilö yrittää lähestyä toista henkilöä tai seurailee ensimmäistä kohdettaan tarkasti ja saa tunnukset selville tarkkailemalla käyttäjän kirjoittamista.

Yleisiä keinoja käyttäjän manipulointiin ovat erilaiset viestit, jotka sisältävät arkaluontoisia kysymyksiä tai tekaistuja käskyjä, jotka näyttävät tulleen käyttäjän omalta esimieheltä. Viestit voivat sisältää myös jonkinlaisia liitteitä tai linkkejä, joiden avaaminen mahdollistaa hyökkäyksen tekemisen. Käyttäjä pyritään saamaan klikkaamaan nämä auki, jonka seurauksena esimerkiksi haittaohjelma pääsee asentumaan käyttäjän laitteelle.

3. SUOJATUN VERKKOKAUPAN RAKENTAMINEN

Verkkokaupan rakentaminen lähtee liikkeelle vaatimusten määrittelyllä ja tietoturvan on syytä olla mukana prosessissa jo alkuvaiheessa, viimeistään suunnitteluvaiheessa. Tällöin täytyy ymmärtää millä tavoin vaatimukset on mahdollista täyttää turvallisesti ja minkälaisia ratkaisuja joudutaan käyttämään. Tätä varten on hyvä peilata OWASP (engl. Open Web Application Security Project) nimisen projektin laatimaa listaa kymmenestä suurimmasta verkko-ohjelmistoihin liittyvästä tietoturvariskistä. Alla olevassa englanninkielisessä Taulukossa 2 on OWASP:n laatima listaus vuodelta 2020 ja vertailuna saman organisaation laatima listaus vuodelta 2017 otettuna kirjasta CEH Certified Ethical Hacker Exam Guide. Tämä osoittaa, kuinka tietoturvassa tapahtuu muutoksia ja asioiden painoarvot vaihtelevat näinkin lyhyessä ajassa. Vuoden 2020 data on muokattu samaan kirjoitusasuun vertailun helpottamiseksi. [20][21]

Taulukko 2. *OWASP top ten web application security risks [20][21].*

Numero	Vuonna 2017	Vuonna 2020
1	Injection flaws	Injection flaws
2	Broken authentication and session management	Broken authentication and session management
3	Cross-site scripting (XSS)	Sensitive data exposure
4	Insecure direct object references	XML external entities (XXE)
5	Security misconfiguration	Broken access control
6	Sensitive data exposure	Security misconfiguration
7	Missing function level access control	Cross-site scripting (XSS)
8	Cross-site request forgery (CSRF)	Insecure deserialization
9	Using components with known vulnerabilities	Using components with known vulnerabilities
10	Unvalidated redirects and forwards	Insufficient logging & monitoring

Taulukosta huomataan, että kahta suurinta riskiä lukuun ottamatta muissa riskeissä on tullut merkittäviä muutoksia kolmen vuoden aikana. Osa on siirtynyt taulukossa ja osa hävinnyt kokonaan uusien korvaavien riskien tieltä. Tämä peilaa hyvin sitä, kuinka teknologia ja kehitystyö ovat muuttaneet toiminnallisuuksia ja vaatimuksia, jolloin vanhat ja uudet riskit vertautuvat uuteen toimintaympäristöön eri tavoilla. Myös asenteissa ja toimintamalleissa on varmasti tapahtunut muutoksia kolmen vuoden aikana, sekä ylläpidon, että vihamielisten toimijoiden puolella.

Suojatun verkkokaupan suunnittelussa ja rakentamisessa onkin tärkeää kartoittaa ja huomioida mahdolliset tietoturvauhat. Tässä kartoituksessa voi hyödyntää apuna Taulukkoa 2, mutta myös muita yleisiä ja ohjelmistokohtaisia tietoturvauhkia. Kartoituksen pohjalta saadaan hyvä kokonaiskuva verkkokaupan riskialttiimmista kohdista, jotka altistavat verkkokaupan vihamielisten toimijoiden hyökkäyksille. Näitä verkkokauppaan kohdistuvia hyökkäyksiä voidaan pyrkiä rajaamaan pienentämällä mahdollisia hyökkäysrajapintoja, eli vihamielisen toimijan mahdollisesti hyödyntämiä heikkouksia verkkokaupasta. Rajaaminen tehdään yleensä rajoittamalla käyttäjän antamien syötteiden määrää ja laatua, sekä sulkemalla ominaisuuksia ja tiedostoja käyttäjien ulottumattomiin.

Toisaalta verkkokaupan suojaamiseksi on mahdollista viritellä erilaisia vihamielistä toimijaa vastaan suunnattuja keinoja erilaisista monitoroinneista aina hunajapurkkeihin. Näistä jälkimmäisen tarkoituksena on huijata vihamielistä toimijaa käyttämään turhaan aikaa ja voimia mielenkiintoiselta vaikuttavaan kohteeseen, joka todellisuudessa ei sisällä mitään oleellista, vaan on rakennettu näyttämään houkuttelevalta hyökkäyskohteelta. Tämän huijauksen paljastuminen vihamieliselle toimijalle saattaa kuitenkin herättää voimakkaita tunteita, jolloin se voi innostaa hyökkäämään entistä kovemmin verkkokauppaa vastaan, joten hunajapurkkia on käytettävä harkiten. [21, s. 165-167]

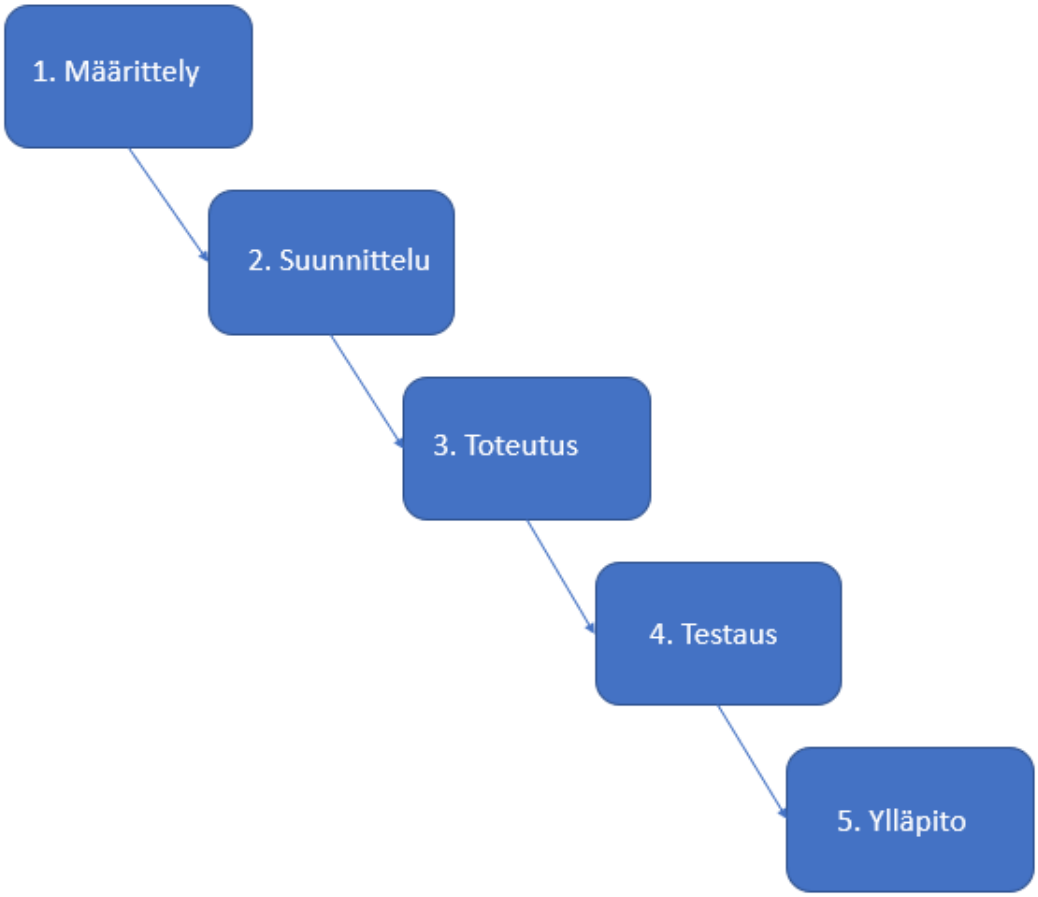
Tässä luvussa käsitellään verkkokaupan rakentamista vaatimusmäärittelystä lähtien aina siihen pisteeseen asti, kunnes verkkokauppa on valmiina testattavaksi. Diplomityöstä johtuvista rajoituksista johtuen, verkkokaupan yksityiskohtaisiin rakennusvaiheisiin ei oteta sen tarkemmin kantaa.

3.1 Vaatimusten määrittäminen

Jokaisen ohjelmistoprojektin alkuvaiheessa määritellään vaatimukset, eli käytännössä se mitä ohjelmistokehityksen lopputuloksena olevan ohjelmiston halutaan tekevän. Tämä pätee myös verkkokauppoihin, sillä on tärkeää ymmärtää mitä verkkokaupassa halutaan myydä, ketkä ovat sen asiakkaita ja miten ylipäänsä verkkokaupan prosessit toimivat.

Verkkokaupan tietoturvan kannalta olennaisimmat vaatimukset liittyvät ensinnäkin palvelimen kielten ja ohjelmistojen versioihin, joilla on jokaisella omat nopeat päivitysaikataulunsa. Tämän jälkeen yleensä määritetään verkkokaupan toimimiseen tarvittavan tiedon laatu ja määrä, sekä katselmoidaan toiminnallisen määrittelyn ominaisuuksien mahdollisesti tuomat tietoturvariskit.

Kuvassa 2 on esitelty yksinkertaistettu ohjelmistokehityksen vesiputousmalli, joka kuvaa kehityksen eri vaiheita alusta loppuun. Jokaisen vaiheen tarkoituksena on antaa riittävät syötteet seuraavalle vaiheelle, jotta tämä seuraava vaihe voi valmistua ja antaa eteenpäin omat syötteensä sitä seuraavalle vaiheelle. Tällöin alkuvaiheiden, varsinkin määrittelyvaiheen, tärkeys korostuu, sillä virheiden aiheuttama vaiva moninkertaistuu myöhemmissä vaiheissa. Tässä diplomityössä ajatuspohjana käytetään vesiputousmallia, vaikka ohjelmistokehityksessä hyödynnetään myös useita muita yleisiä malleja.



Kuva 2. *Yksinkertaistettu ohjelmistokehityksen vesiputousmalli.*

Kuva 2 havainnollistaa siis yksinkertaista vesiputousmallia, josta on karsittu pois yksityiskohtaisempia vaiheita. Tähän yksinkertaistettuun malliin kuuluu aluksi ohjelmiston määrittely ja sen suunnittelu, joiden pohjalta tehdään ohjelmiston toteutus. Valmiin toteutuksen jälkeen tämä kyseinen toteutus testataan ja kun testaus on hyväksytysti suoritettu, voidaan ohjelmisto hyväksyä julkaistavaksi tarkoituksenmukaiseen käyttöönsä ja se siirtyy samassa yhteydessä ylläpitovaiheeseen.

3.2 Laitteiden ja ohjelmistojen valinta

Verkkokauppaa varten valittavien laitteiden ja ohjelmistojen täytyy palvella verkkokaupan tarpeita ennalta suunnitellulla tavalla, eli käytännössä näiden täytyy vastata vaatimusmäärittelyn pohjalta saatuihin vaatimuksiin. Tämä siis tarkoittaa sitä, että vaatimuksista on löydettävä omat kohtansa laitteiston vaatimuksiin ja vastaavasti ohjelmistojen vaatimuksiin. Yleisesti verkkokaupan laitevaatimukset painottuvat palvelimen puolelle, jolloin käyttöön halutaan riittävän tehokas laitteisto, jolla on tarkoituksenmukainen suojaus. Samalla saatetaan määrittää myös verkkoon liittyvää laitteistoa, kuten palomuureja tai verkkolaitteistoa yleensä.

Ohjelmistoista vaatimusten pohjalta olennaisimpia ovat käytännössä palvelimen ohjelmistot ja itse verkkokaupan ohjelmistot. Palvelimen osalta vaatimusmäärittelyssä listataan mitä versioita erilaisista kielistä ja ohjelmistoista palvelimen täytyy tukea, kuten esimerkiksi PHP:n tuettu versionumero. Näin ollen vastataan näiden versioiden osalta tietoturvan tarpeisiin.

Itse verkkokaupan ohjelmistoilla on aina vaatimuksia ohjelmointikielten ja palvelinohjelmistojen versioista. Näiden avulla voidaan aluksi kartoittaa ne verkkokaupat, jotka toimivat määritellyissä rajoissa. Seuraavaksi katsotaan toiminnallisen määrittelyn pohjalta mitkä ohjelmistot vastaavat parhaiten määrittelyssä asetettuihin tarpeisiin, sekä kaikkiin muihin määritysvaiheessa esitettyihin tarpeisiin, kuten tietoturvan ja ylläpidettävyyden tarpeisiin. Näiden pohjalta valitaan lopuksi käytettävä verkkokauppaohjelmisto, jonka tulisi nyt täyttää kaupalle asetettavat olennaiset vaatimukset.

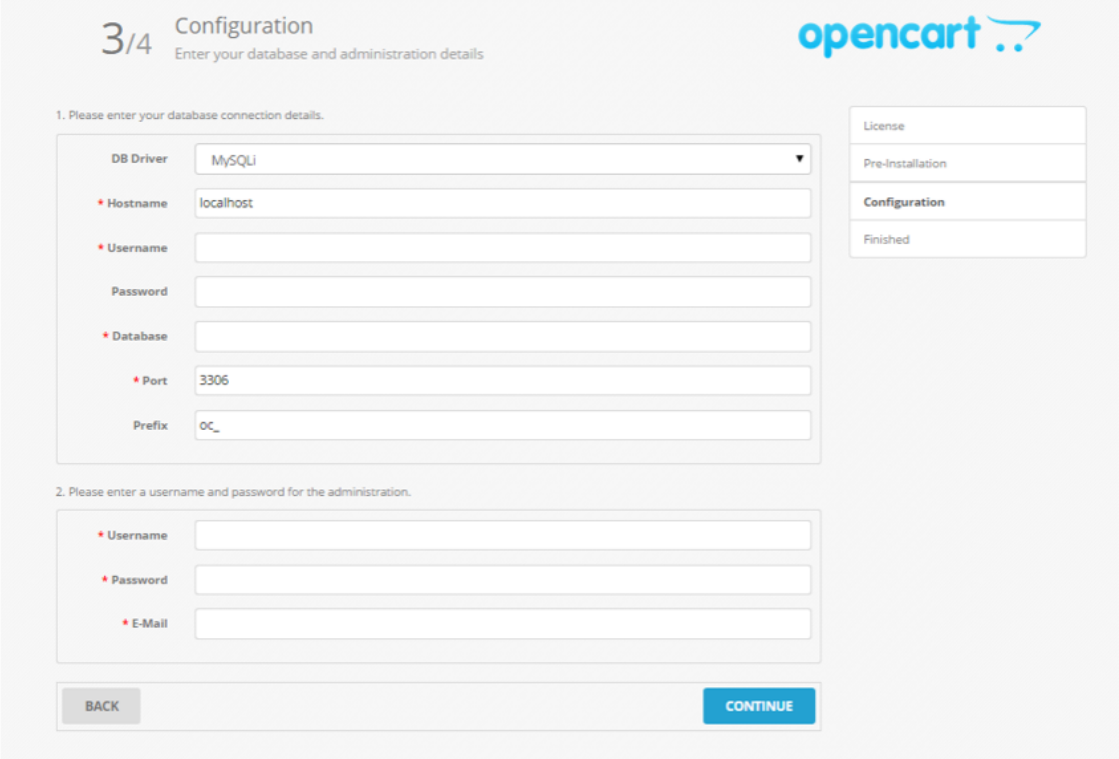
3.3 Ohjelmistojen asennus ja konfigurointi

Ohjelmistojen valitsemisten jälkeen tehdään niiden asennus valitulle palvelimelle. Tässä vaiheessa on usein myös lokaalin ympäristön, eli ohjelmistokehittäjän tietokoneen tai vastaavan ympäristön, pystytys. Jätetään lokaalin ympäristön pystyttäminen kuitenkin pois tämän diplomityön aihepiiristä, sillä se on samankaltainen palvelimelle asentamisen kanssa. Samalla voidaan olettaa palvelimen ohjelmistojen tulevan valmiiksi asennettuna

pakettina, jolloin varsinaisen verkkokaupan ohjelmistojen asentaminen ja konfigurointi on mukana tämän diplomityön aihepiirissä.

Verkkokauppaohjelmiston asentaminen omalle palvelimelle on yleisimmissä avoimen lähdekoodin ohjelmistoissa tehty käyttäjälle helpoksi, jolloin yleensä tiedostojen lataaminen palvelimelle, asennusprosessin käynnistäminen ja tarvittavien syötteiden antaminen asennuksen aikana riittävät verkkokauppaohjelmiston onnistuneen asennuksen suorittamiseen. Tämä diplomityö ei ota kantaa sellaisiin verkkokaupparatkaisuihin, joita kolmannen osapuolen edustajat myyvät valmiina tuotepaketteina asennettuina palvelimilleen.

Asennusvaiheessa verkkokauppaohjelmisto kysyy olennaisia tietoja verkkokaupan toimintaan ja tuleviin käyttäjiin liittyen. Verkkokauppaohjelmistosta riippuen, asennuksen yhteydessä käyttäjältä kysyttävät syötteet saattavat sisältää jo tietoturvaan liittyviä ratkaisuja, kuten tulevatko TLS ja HTTPS käyttöön, sekä estetäänkö tiedostolistauksen tekeminen. Tämä ei kuitenkaan pelkästään vielä riitä, vaan tarvitaan monia muita asennuksen jälkeisiä konfigurointeja, jotta haluttu lopputulos saataisiin aikaiseksi. Nämä konfiguroinnit liittyvät tiedostojen ja kansioiden käyttöoikeuksiin, sekä erilaisiin verkkokauppaohjelmiston ominaisuuksiin ja sen käyttäjäprofiileihin. Alla oleva Kuva 3 esittää OpenCartin asennusvaiheen kysymyksiä tietokannasta ja pääkäyttäjän tunnusten luomisesta.



Kuva 3. *OpenCartin asennusvaiheen kysymyksiä [8].*

Yleensä jokainen verkkokauppaohjelmisto tarvitsee toimiakseen tietokannan tai useamman tietokannan eri tarkoituksiin. Yksi tietokanta sisältää monta taulua, johon tallennetaan verkkokaupan eri osa-alueiden ja toimintojen tietoja. Nämä tiedot sisältävät niin tuotteisiin, kuin käyttäjiin liittyviä arkaluonteisiakin tietoja. Tämän vuoksi tietokannat kiinnostavat myös vihamielisiä toimijoita, sillä arkaluonteisista tiedoista voi päästä hyötymään jollain tavalla. Tämä tuo verkkokaupan ylläpitäjälle haasteita, sillä käyttäjän arkaluonteiset tiedot on pystyttävä suojaamaan mahdollisimman hyvin.

Verkkokauppaohjelmistoissa suurin osa tietokannasta on yleensä kirjoitettu selkokielellä, joten kuka tahansa tietokantaan pääsevä voi ymmärtää tietokannan sisällön. Osa arkaluonteisimmista asioista, kuten salasanat on kuitenkin yleensä suojattu käyttäen suojausalgoritmia. Tällöin käyttäjän verkkokauppaohjelmistoon antama syöte muutetaan salaamalla kryptattuun muotoon tietokantaan tallennusta varten, eikä tämä ole enää luettavissa selkokielisenä. Verkkokaupan suunnittelussa ja konfiguroinnissa onkin syytä ottaa huomioon arkaluonteisten tietojen tallennus salattuna tietokantaan.

Tietokannat on syytä suojata myös muilla verkkokauppaohjelmiston konfiguroinneilla. Pääasiassa tämä tarkoittaa käyttäjän kenttiin ja lomakkeisiin antamien syötteiden rajoittamista esimerkiksi pituudella, sekä kiellettyjen merkkien ja tiedostomuotojen määrittämisellä. Tällöin vihamieliset toimijat eivät pääse antamaan syötekenttiin käskyjä tietokannalle ja eivät näin ollen pääse helposti tietokantaan käsiksi.

Myös kaikki verkkokaupan kävijöille lähetettävät automaattiset sähköpostit on syytä konfiguroida heti alussa, sillä edellisessä luvussa mainitulla tavalla voi vihamielinen taho päästä käsiksi verkkokaupan kannalta olennaiseen tietoon tai esiintyä verkkokauppana hyödyntäen käytössä olevaa sähköpostin mallipohjaa ja haltuunsa saamia tietoja. Tässä tilanteessa verkkokaupan oikea asiakas ei välttämättä enää pysty helposti erottamaan tuleeko viesti oikeasta verkkokaupasta vai vihamieliseltä toimijalta.

Asennusvaiheessa verkkokauppaan lisätään tarpeen mukaan myös erilaisia integraatioita, kuten yhteydet maksupalveluun ja kuljetusyritykseen. Yleensä näille toiminnoille on olemassa valmiit lisäosat verkkokauppaohjelmistoon, jolloin tietoturvan kannalta olennaiseksi jää luotettavan lisäosan löytäminen ja sen oikeanlaisten konfigurointien tekeminen, sekä suojaamisesta huolehtiminen verkkokaupan päässä.

Pelkän verkkokauppaohjelmiston konfiguroinnin lisäksi on avoimen lähdekoodin verkkokauppaohjelmistoihin hyvä tehdä muita yleisiä muutoksia, joita ei välttämättä ole ohjeistettu ohjelmiston yhteydessä. Yleisesti on suositeltavaa pyrkiä välttämään oletusarvoisia

käyttäjätunnuksia tai kansion ja tietokannan nimiä, sillä näitä luodaan jokaisessa verkkokauppaohjelmistossa tietyllä logiikalla tai ne ovat oletusarvoisesti jotain yleisesti tiedettyä.

Samalla on olennaista miettiä, mitkä osiot verkkokaupassa ovat tietokannan lisäksi tärkeimpiä suojauskohteita. Näitä ovat yleensä hallintapaneelin kansio, joka onkin hyvä nimetä uudelleen, sekä tiedostojen ja kansioiden chmod-arvot (engl. change mode), jotka määrittävät kyseisiin tiedostoihin ja kansioihin kohdistuvat oikeudet. Alla oleva Taulukko 3 havainnollistaa chmod-arvoja tarkemmin. Taulukossa r, w ja x tarkoittavat kyseisen oikeuden olemassaoloa, eli r tarkoittaa lukuoikeutta, w puolestaan kirjoitusoikeutta ja x suoritusoikeutta. [11]

Taulukko 3. *Chmod-arvojen merkitys [11].*

Oktaaliarvo	Lukuoikeus (arvo 4)	Kirjoitusoikeus (arvo 2)	Suoritusoikeus (arvo 1)
7	r	w	x
6	r	w	-
5	r	-	x
4	r	-	-
3	-	w	x
2	-	w	-
1	-	-	x
0	-	-	-

Taulukon perusteella nähdään miten erilaiset luku-, kirjoitus- ja suoritusoikeuksien yhdistelmät luovat erilaiset oktaaliarvot. Oktaaliarvot lasketaan näiden oikeuksien perusteella taulukon osoittamien arvojen avulla. Tämä oktaaliarvo lasketaan kolmelle eri käyttäjäryhmälle, joita ovat käyttäjä, ryhmä ja muut. Näin ollen saadaan kolme oktaaliarvoa, jotka kirjoitetaan peräkkäin ja näin ollen saadaan lopullinen chmod-arvo. Tästä esimerkkinä kaikille käyttäjäryhmille kaikki oikeudet salliva 777. [11]

Myös esimerkiksi tiedostolistauksen tekemistä on hyvä rajoittaa ja ottaa käyttöön selkokieliset URL-osoitteet (engl. Uniform Resource Locator), jolloin tiedostojen sijainnit ja hakemistorakenne eivät ole suoraan näkyvillä. Selkokielisten URL-osoitteiden käyttö auttaa myös hakukonenäkyvyyden parantamisessa.

Osa verkkokauppaohjelmiston kansioista voidaan myös tarpeen mukaan sulkea salasanan ja IP-suojauksen taakse, jolloin esimerkiksi hallintapaneelin käyttö voidaan rajata tiettyyn alueeseen, kuten toimistolle, ja vain rajatut käyttäjät pääsevät toimistolta siihen käsiksi annetuilla tunnuksilla. Nämä toimenpiteet, sekä jossain määrin myös tiedostojen ja kansioiden oikeuksiin liittyvät muutokset saattavat vaikeuttaa valmiin verkkokauppaohjelmiston testaamista, joten kyseiset toimenpiteet on syytä ajoittaa oikein sujuvan testaamisen varmistamiseksi.

3.4 Testaaminen

Verkkokaupan testaamisen kokonaisuuteen kuuluu myös verkkokaupan tietoturvan testaaminen. Koko verkkokaupan testaamisen suunnittelu aloitetaan jo varhaisessa vaiheessa, jolloin verkkokaupan toteutuksen valmistuttua on selkeästi tiedossa mitkä asiat täytyy testata ja minkälainen lopputulos on syytä saada aikaiseksi.

Tietoturvan testaamisessa on hyödyksi käyttää siihen erikoistuneita testaajia, sillä osa testauksessa käytettävistä testitapauksista voi sisältää vaatimuksia tietoturvan perustaidoille tai toisaalta verkkokaupassa käytetyn ohjelmointikielen tarkkaa tuntemusta. Testauksen suorittamiseen on yleensäkin hyvä käyttää eri henkilöitä, kuin varsinaisen toteutuksen tekijöitä. Tämä perustuu siihen, että toinen henkilö havaitsee helpommin toisen henkilön mahdolliset virheet ja näin ollen verkkokaupasta tulee lopulta turvallisempi.

Tietoturvan testaaminen voi myös olla luonteeltaan erilaista muuhun testaamiseen verrattuna, sillä tietoturvan testaamisessa ei pyritä vain toteamaan, että testattava asia toimii tai ei toimi määritellyllä tavalla, vaan sen tarkoituksena on kartoittaa mahdollisia tietoturva-aukkoja ja tehdä näin ollen verkkokaupasta mahdollisimman turvallinen.

Neljäs luku käsittelee verkkokauppaan liittyvää testausta tarkemmalla tasolla.

3.5 Käyttäjien ohjeistaminen

Kuten toisessa luvussa todettiin, käyttäjien rooli on suunnattoman tärkeä turvallisen verkkokaupan ylläpitämisessä, sillä käyttäjien aiheuttamat virheet ja heidän epätietoisuutensa ovat helpoin tapa kiertää verkkokaupan tietoturvaa. Verkkokaupan voi suojata tekniseltä kannalta äärimmäisen hyvin, mutta jos tietyillä käyttäjäoikeuksilla varustetun henkilön käyttäjätili saadaan haltuun tai käyttäjä saadaan manipuloitua tekemään virheellisiä asioita, niin paraskaan tekninen suojaus ei auta loputtomiin. Käyttäjillä tässä tapauksessa tarkoitetaan niin verkkokaupan ylläpitoa ja muuta henkilöstöä, kuin verkkokaupassa vierailevia asiakkaita. Ohjeistamalla jokainen taho oikealla tavalla, voidaan vähentää riskiä verkkokaupan tietoturvan vaarantumisesta.

Ohjeistaminen voidaan suorittaa monella eri tavalla, kuten dokumentoimalla selkeät ohjeet, kouluttamalla verkkokaupan parissa toimivat käyttäjät tai ohjailemalla käyttäjiä oikeisiin ratkaisuihin verkkokaupan toteutuksella.

Verkkokaupan tietoturvasta voidaan dokumentoida oma erillinen ohjeistuksensa tai se voidaan liittää omana osionaan verkkokaupan muuhun ohjeistukseen. Muusta ohjeistuksesta poiketen, sen on hyvä olla ytimekäs ja toimia enemmän käyttäjää muistuttavana dokumenttina, kuin jokaisen ominaisuuden esittelevänä ja listaavana ohjeena. Tietoturvaan liittyvään ohjeistukseen kuuluu olennaisena osana kirjautumistietojen, eli tunnusten ja salasanojen, käytön ohjeistaminen. Tämä ohjeistaminen voi sisältää kirjautumistietojen laadullisia määrityksiä, kuten pituus ja sisältö, mutta myös niiden säilyttämiseen ja käyttämiseen liittyviä ohjeistuksia.

Maksujärjestelmiin erikoistunut yritys Stripe listaa tietoturvaan keskittyvässä Increment Security -julkaisussaan käyttäjien salasanoihin liittyviä yleisiä ongelmakohtia, joita ovat saman salasanan käyttäminen monessa eri palvelussa, sekä salasanan kirjoittaminen muistiin joko yksittäiselle paperilapulle tai erilliseen salasanojen muistikirjaan. Näiden käytäntöjen estämiseksi julkaisussa ehdotetaan muistisääntöjä tai salasanojen hallintaan tehtyä ohjelmistoa, jotka luonnollisesti tulee tässä yhteydessä dokumentoida selkeästi verkkokaupan ohjeissa. [7]

Salasanan muistiin kirjoittamisesta on nostettu esille räikeänä tapauksena Havaijilla paikallisessa virastossa tapahtunut vahinko. Tässä tapauksessa julkiseen jakeluun päätynyt valokuva sisälsi kuvatun henkilön lisäksi näkymän viraston käyttämästä järjestelmästä, sekä näyttöön liimatun ja selkeästi kuvasta luettavissa olevan muistilapun, johon oli kirjoitettu kyseisen järjestelmän salasana [10].

Ohjeistuksen lisäksi myös koulutuksella voidaan saada aikaan tietoturvan kannalta hyviä tuloksia esittelemällä käytännössä verkkokaupan vaaratekijät varoittavalla sävyllä, jolloin ne saattavat jäädä koulutettavan yleisön mieleen pelkkää käyttöä ohjeistavaa dokumenttia paremmin. Myös käyttäjien omakohtaiset kokeilut ja mahdollisuus testata hallitusti ongelmakohtia, lisäävät koulutuksen ydinviestin tehokkuutta ja mieleenpainuvuutta.

Verkkokaupan käyttäjää voidaan myös ohjailla erilaisilla tavoilla, kuten lisäämällä ohjetekstejä verkkokaupan toimintojen yhteyteen tai huomautusikkunoita tärkeisiin toimenpiteisiin, jolloin oleellisten toimintojen käyttäminen varmistetaan uudelleen käyttäjältä. Tällaisella varmistamisella saadaan minimoitua käyttäjän epähuomiossa tekemiä virheitä.

Käyttäjien toiminnan rajoittaminen on tehokas keino ennaltaehkäistä tietoturvauhkia. Toimintaa voidaan rajoittaa jakamalla käyttäjät erilaisiin ryhmiin, joille annetaan erilaisia käyttöoikeuksia. Näitä ryhmiä voivat olla esimerkiksi verkkokaupan ylläpitäjät ja tilausten

käsittelijät. Tässä tapauksessa pääsy verkkokaupan ylläpitoon voidaan rajata kirjautumisella tai vahvemmin vaikkapa IP-osoitteeseen pohjautuvilla rajoituksilla. Käyttäjien antamien syötteiden määrittäminen ja niiden rajoittaminen on myös tärkeä osa verkkokaupan tietoturvaa. Tähän sisältyy syötteiden pituuksien ja sisältöjen määritteleminen kirjautumistietojen, sekä kenttien ja lomakkeiden osalta.

Tässä luvussa käsiteltiin verkkokaupan rakentamista ja nyt verkkokaupan voidaan olettaa olevan toteutukseltaan valmis. Seuraavassa luvussa käsitellään valmiin verkkokaupan testaamista ja sen pohjalta syntyvien korjausten tekemistä.

4. TIETOTURVAN TESTAAMINEN JA KORJAUKSET

Tässä luvussa testataan edellisessä luvussa valmistunutta verkkokaupan toteutusta. Testauksen avulla selvitetään, onko verkkokaupan suojaus toivotulla tasolla, eli vastaako se ensinnäkin alussa asetettuja vaatimusmäärittelyjä ja toisaalta löytyykö tietoturvan testauksessa vielä jotain muuta huomionarvoista. Jos testauksessa paljastuu jotain huomioitavaa, nämä huomiot kirjataan ja niille tehdään yleensä jonkinlaiset korjaukset. Korjaustarve voidaan luokitella kriittisyyden pohjalta ja joidenkin huomioiden osalta voidaan myös päätyä ratkaisuun, jossa korjaamista ei nähdä verkkokaupan kannalta välttämättömänä.

Testauksessa käytetään pohjana testitapauksia, joissa testaaja käy läpi vaatimusmäärittelyn pohjalta luodut olennaiset testausvaiheet. Testitapauksissa on yksiselitteiset ohjeet, kuinka kyseisen testitapauksen testaus suoritetaan ja kuinka siitä edetään jokaiseen testitapauksen kohtaan loogisesti määrätyssä järjestyksessä. Testitapauksia on useita ja myös testitapausten välillä on määritelty looginen etenemisjärjestys testitapauksesta toiseen.

Tässä diplomityössä testaajaksi kutsutaan nyt pääsääntöisesti vain verkkokaupan tietoturvan testaavaa tahoa, vaikka testaajia on ohjelmistoprojekteissa moneen eri testauksen osa-alueeseen. Jokaisen yksittäisen läpikäydyn testitapauksen jälkeen, kaikki kyseisen testitapauksen suorittamisen aikana tehdyt havainnot kirjataan ylös ja näiden havaintojen perusteella testitapaus joko hyväksytään tai hylätään.

Hyväksyminen voi käytännössä tapahtua vain silloin, kun testitapaukset voidaan suorittaa ennalta määrätyllä tavalla läpi ja ne tuottavat oletetun lopputuloksen. Muutoin testitapaukset hylätään ja hylkäyksen syy kuvataan testitapaukseen. Hyväksytty testitapaus kertoo, että kyseinen osuus verkkokaupasta on valmis käytettäväksi ja se jää odottamaan muiden testitapausten valmistumista. Hylätty testitapaus puolestaan palaa verkkokaupan toteuttaneelle taholle korjattavaksi dokumentoitujen kommenttien perusteella. Näiden korjausten jälkeen testitapaus palaa uudelleen testattavaksi samalle testaajalle, joka jälleen hyväksyy tai hylkää testitapauksen, eli tässä tapauksessa havaitun virheen korjauksen.

Prosessi jatkuu tämän testitapauksen ja kaikkien muiden testitapausten osalta samalla tavalla siihen saakka, kunnes kaikki testitapaukset saadaan hyväksytyiksi tai testauksessa löydetyt virheet on todettu matalan prioriteetin korjauksiksi, jolloin ne saatetaan jättää joko myöhempään korjaukseen tai lopulta kokonaan korjaamatta.

Tietoturvatestausta voidaan tehdä manuaalisesti tai siinä voidaan käyttää siihen kehiteltyjä työkaluja, kuten Metasploit Framework, jolla voi hyvin laaja-alaisesti kirjoittaa, testata ja suorittaa hyökkäyskoodeja tietoturvan testaamiseksi ja kohteeseen perehtymiseksi. Tällaiset työkalut ovat kuitenkin hyödyllisiä myös vihamielisille toimijoille, jotka voivat hyötyä väärissä tarkoituksissa tehokkaista työkaluista. Paras keino niitä vastaan suojautumiselle onkin verkkokaupan testaaminen näillä työkaluilla vihamielisten toimijoiden käyttämillä menetelmillä. [21, s. 202, 233-234, 248]

Laaja-alaisten testausohjelmistojen lisäksi on olemassa suuri joukko erilaisia tiettyihin testauskohteisiin erikoistuneita ohjelmistoja, joita voidaan käyttää niin tietoturvan testaamiseen, kuin hyökkäyksiin. Näitä ohjelmistoja on olemassa käyttötarpeen mukaisesti keskittyen erilaisiin ohjelmistoihin, verkkoihin ja laitteisiin.

Seuraavaksi käsitellään tarkemmin testaamista eri osa-alueilla, sekä näihin liittyviä havaittuja korjaustarpeita ja niiden käytäntöjä.

4.1 Ohjelmistot

Verkkokauppaohjelmiston ja siihen liittyvien lisäosien tai muiden sidonnaisten ohjelmistojen testaaminen on tärkeä vaihe testauksessa, sillä nämä ohjelmistot käsittelevät verkkokaupan ydintoimintoja. Tämä tarkoittaa sitä, että arkaluontoisten tietojen käsittely ja maksamiseen liittyvät toimenpiteet hoidetaan näissä ohjelmistoissa, joten ongelmatilanteiden syntyminen saattaa aiheuttaa tietoturvauhkia tai horjuttaa verkkokaupan asiakkaan luottamusta.

Verkkokaupan ohjelmistojen testaamiseen on olemassa erilaisia vaihtoehtoja, mutta korkealla tasolla se jakaantuu käytännössä automatisoituun ja manuaaliseen testaamiseen. Tässä diplomityössä rajataan pois tarkempi erilaisten testausmenetelmien käsittely ja keskitytään suoranaisesti tietoturvan testaamiseen.

Automatisoidussa testauksessa voi olla käytössä sitä varten tuotettu ohjelmisto tai testaus voi tapahtua koodipohjaisesti, varsinkin monimutkaisten kaavojen ja laskutoimitusten osalta. Automatisoidussa testauksessa joudutaan yleensä luottamaan siihen, että ohjelmisto tai koodi on toteutettu oikein ja testattu riittävästi, jolloin verkkokaupan testaa-

misen lopputuloksen täytyisi pitää paikkaansa. Tietysti testausvirheissä tai väärissä lopputuloksissa voidaan huomata, että ohjelmisto tai koodi ei toiminut jostain syystä oikein, mutta näiden havaitseminen testausvaiheessa voi olla hyvin hankalaa.

Manuaalisessa testaamisessa käydään testitapaukset läpi käsin, esimerkiksi verkkokauppaa klikkailemalla, antamalla syötteitä tai muulla tavoin verkkokaupan ominaisuuksia testaamalla. Manuaalisen testaamisen tuloksena nähdään yleensä verkkokaupan toiminnallisuuksiin liittyviä tuloksia, joiden on täytettävä testitapauksissa määritellyt vaatimukset.

Verkkokauppaohjelmiston tietoturvan testauksen tulisi sisältää varsinkin ohjelmistoon itseensä kohdistuvien yleisimpien tietoturvauhkien testauksen. Tietoturvaan keskittynyt yritys Astra IT ylläpitää listaa OpenCart -verkkokauppaohjelmiston yleisimmistä tietoturvauhista, jotka on koottu seuraavaan Taulukkoon 4. [16]

Taulukko 4. *OpenCartin yleisimmät tietoturvauhat [16].*

Yleisimmät uhat
1. Cross-Site Request Forgery
2. Server Side Request Forgery
3. Directory Traversal
4. SQL Injection
5. Cross-Site Scripting

Taulukosta nähdään, että OpenCartiin kohdistuvat tietoturvauhat ovat hyvin pitkälti linjassa yleisien verkkosivustoihin kohdistuvien tietoturvauhkien kanssa, jotka esitettiin aiemmin Taulukossa 2. Näin ollen voidaan todeta, ettei testauksessa sovi unohtaa yleisiä tietoturvauhkia, vaikka jokaisessa ohjelmistossa onkin vielä niiden lisäksi omat tietoturvauhkansa ja verkkokauppaohjelmistokohtainen tuntemus onkin testauksen suunnittelussa erittäin tärkeää.

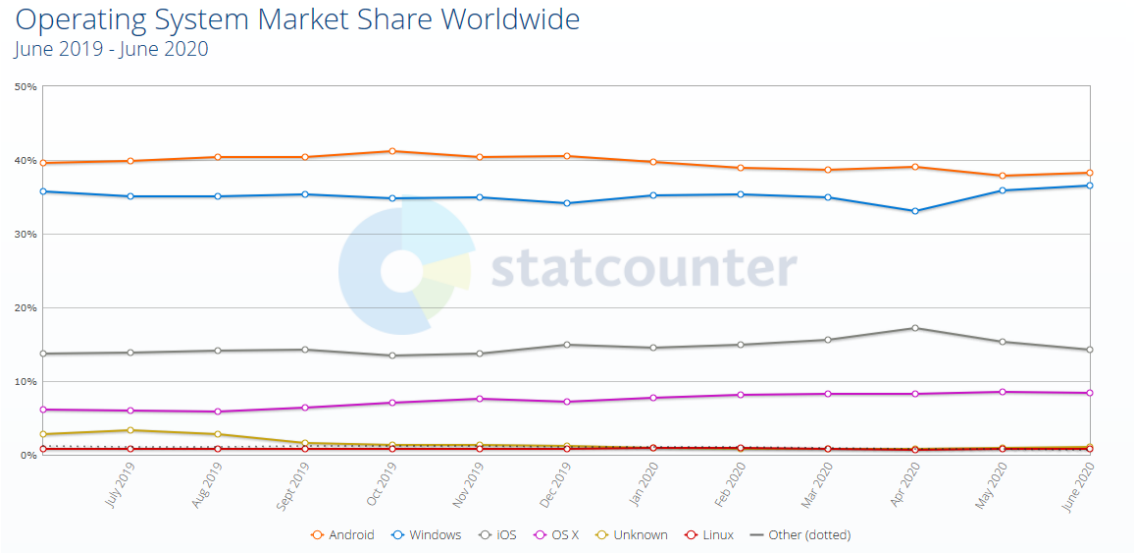
Verkkokauppaohjelmiston tietoturvan testaaminen suoritetaan käytännössä alkuvaiheessa luotujen testitapausten pohjalta, joissa testaaja ohjeistetaan käymään läpi tietyt testaustoimenpiteet määrätyssä järjestyksessä. Pelkän ohjelmiston tietoturvan testaamisen lisäksi tähän kuuluvat ohjelmiston näkökulmasta myös verkkokauppaohjelmistoon liittyvien integraatioiden ja verkkokauppaohjelmistosta lähtevien sähköpostien tietoturvan testaaminen.

4.2 Laitteet

Verkkokaupan tietoturvan kannalta käyttäjien yksittäisten laitteiden testaus ei ole olennaisessa osassa, mutta verkkokauppa olisi kuitenkin hyvä testata riittävän laajalla laitekannalla, jolloin voidaan todeta verkkokaupan toimivan niillä oikein, eikä kriittisiä ongelmatilanteita ilmaannu. Nämä kriittiset ongelmatilanteet voivat lähinnä paljastaa jotain olennaista verkkokaupasta tai antaa verkkokaupassa vierailevan laitteen käyttäjän luoda erilaisia syötteitä verkkokauppaan, jolloin verkkokauppa altistuu hyökkäysuhalle.

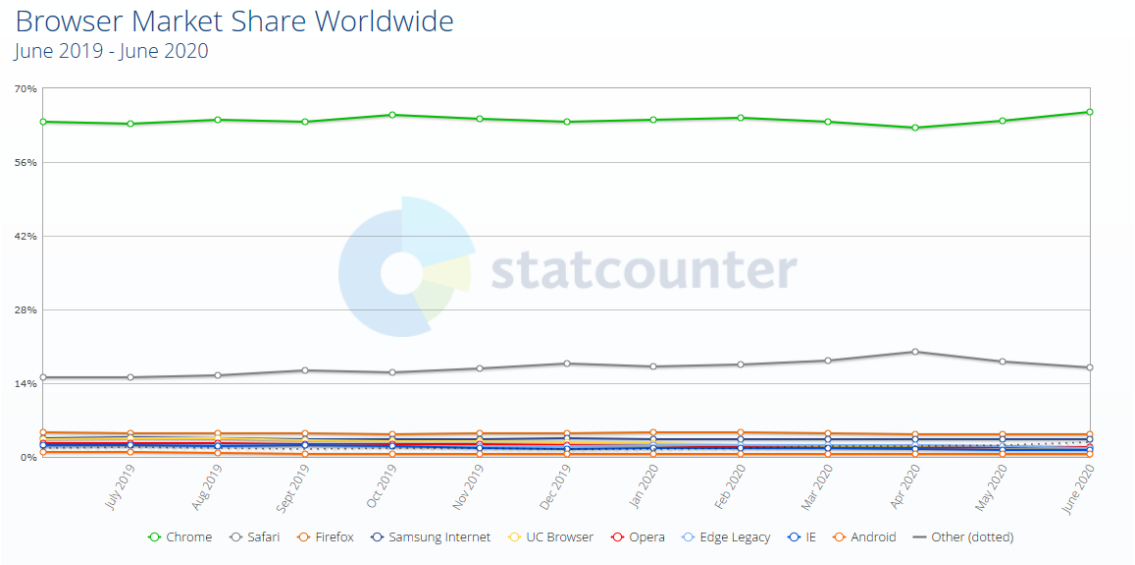
Tässä tapauksessa laitteet sisältävät verkkokaupan hallinnan käyttämiseen liittyvän laitteiston, eli henkilökunnan käyttämät tietokoneet ja mobiililaitteet. Ylläpidetyn palvelimen osalta riittää tämän diplomityön puitteissa palvelimen komponenttien ja sen tarjoamien ohjelmistoversioiden vertaaminen vaatimusmäärittelyssä mahdollisesti annettuihin versioihin.

Käytännössä laitteiden testaus sisältäisi ajanhetkeen sopivan yleisimpien laitteiden listan käyttöjärjestelmineen ja selaimineen, jolloin testauksella katettava prosenttiosuus näistä on riittävän suuri. Tällainen listaus löytyy ilmaiseksi vaikkapa tilastodataa tarjoavan Statcounterin palvelun kautta. Alla olevat Kuva 4 ja Kuva 5 esittävät esimerkkeinä verkkosivuilta maailmanlaajuisesti kerättyä dataa käytetyimmistä käyttöjärjestelmistä ja verkkoselaimista. [14][1]



Kuva 4. *Käyttöjärjestelmien maailmanlaajuiset markkinaosuudet [14].*

Kuvan 4 havainnollistaman tilaston pohjalta voidaan olettaa testaukseen sopiviksi laitteiksi sellaiset, joiden käyttöjärjestelmänä on Android, Windows, iOS tai OS X. Tällöin katetaan Statcounteria käyttävien sivustojen keräämän datan mukaan 97,5% maailmanlaajuisesta laitekapasiteetista. [14]



Kuva 5. *Selainten maailmanlaajuiset markkinaosuudet [1].*

Samoin voidaan olettaa Kuvan 5 havainnollistaman tilaston pohjalta, että testaukseen sisällytettävät selaimet olisivat Chrome, Safari, Firefox ja Samsung Internet, jolloin Statcounterin mukaan katettaisiin 89,97% laitteista maailmanlaajuisesti. [1] Samalla täytyy kuitenkin todeta, ettei yleisimpiin käyttöjärjestelmiin ja selaimiin keskittyminen tuo täysin kattavaa testaustulosta verkkokaupalle, mutta käytännön kannalta jokaisen käyttöjärjestelmän ja selaimen versioiden yhdistelmän testaaminen tulee mahdottomaksi ja todennäköisesti turhaksi työksi. Näin ollen tyydytään siis mahdollisimman kattavaan testauskokonaisuuteen ja pidetään sitä riittävänä.

Laitteiden ja niiden ohjelmistojen päivityksillä voidaan parantaa tietoturvaa tunnettujen haavoittuvuuksien osalta. Tästä johtuen testauksessa olisi syytä määrittää verkkokaupan henkilöstön käyttämät laitteistot ja ohjelmistot, jolloin vanhentuneet laitteet ja ohjelmistoversiot karsittaisiin pois käytöstä. Tämä pitäisi käytännössä toteuttaa keskitetysti hallitulla päivitysohjelmalla kohdennetulle henkilöstölle, jolloin henkilöstölle ei tule varaa valita asentavatko päivityksen vai eivät.

Laitteiden sisältämissä fyysisissä piireissä saattaa myös piillä erilaisia tietoturvauhkia, eikä niiden varalta ole helppoa varautua ennalta käsin. Tämän vuoksi verkkokaupan testaaminen on hyvin hankalaa ulottaa näin syvälliselle tasolle, vaikka piirien kautta onkin lopulta mahdollista altistaa koko verkkokauppa vihamielisen toimijan käsiin. Tällainen uhka on toteutunut esimerkiksi taiwanilaisen komponenttivalmistaja MediaTekin piirien kohdalla, kun tietoturva-aukon avulla on ollut mahdollista asentaa Android-laitteeseen ohjelmia käyttäjän huomaamatta [19].

Verkkokaupassa tämä olisi mahdollistanut sen, että testauksessa suojatuksi osoittautunut verkkokauppa olisi saatu haltuun ylläpidon Android-laitteen kautta tunnusten kaappaamisen avulla. Se olisi tarkoittanut koko verkkokaupan sisällön ja asiakkaiden arkaluontoisten tietojen vuotamisen vihamieliselle toimijalle.

4.3 Verkot

Verkkojen aiheuttamien tietoturvauhkien testaaminen ei ole kovin yksiselitteistä, sillä palvelimen verkkoyhteyksien lisäksi verkkokaupan ylläpidon ja asiakkaiden verkkoyhteydet tuovat omat uhkansa tietoturvalle, eikä aina voida ennalta olla varmoja minkälaisista verkoista verkkokauppaan tullaan.

Palvelimien osalta riittää usein, että tarkastellaan jo valmiiksi hyvin hoidetun ulkoistetun palveluntarjoajan ratkaisua ominaisuuksien tasolla ja varsinainen testaaminen jää sivuun, jos ominaisuudet täyttävät asetetut vaatimukset. Vaatimuksissa voi olla määrityksiä kulunvalvonnasta ja verkon suojaamisesta, jolloin nämä kuuluvat testauksen piiriin verkon tietoturvan näkökulmasta.

Palvelin saattaa myös olla omatekoinen tai sijaita ennalta tuntemattomassa kohteessa, jolloin kulunvalvonta ja verkon suojaaminen tulisi testata. Aina tämä ei ole mahdollista, joten silloin tulisi selvittää mahdollisimman tarkasti, miten kulunvalvonta ja verkon suojaaminen toteutetaan. Selvitykset tai mahdolliset testaukset olisi syytä tehdä siksi, että ulkoisen verkon kautta palvelimeen kohdistuu suurin potentiaali uhkatekijöille. Toisaalta vihamieliselle toimijalle on helpointa päästä fyysisesti kiinni palvelimen lähiverkkoon ja pääsemällä palvelimen kanssa samaan tilaan, voi palvelimesta löytyä oleellisia lisätietoja, jolloin kulunvalvonta on oleellisessa osassa tietoturvaa.

Monesti ulkoisen verkon kautta tulevat hyökkäykset kohdentuvat itse verkkokauppaohjelmistoon ja hyödyntävät sen tarjoamia aukkoja tai mahdollisuuksia, mutta ne on käsitelty erikseen aiemmin kohdassa 4.1. Myöskin käyttäjiin, eli tässä tapauksessa verkkokaupan ylläpitäjiin, muuhun verkkokaupan henkilöstöön ja asiakkaisiin liittyvät kohdat

käsitellään laajemmin seuraavassa kohdassa 4.4. Tässä vaiheessa käsitellään kuitenkin vielä käyttäjien verkkoihin liittyvien uhkien testaaminen.

Verkkokaupan ylläpidon ja muun henkilöstön osalta on tärkeää tietää mistä he tulevat yhdistämään käyttämänsä laitteet tietoverkkoon omissa työtehtävissään. Tällöin toimiston ja kotitoimiston verkkojen tulee täyttää alussa määritetyt vaatimukset, jolloin testaaminen voidaan suorittaa käytännössä vertaamalla vaatimuksia olemassa olevaan tilanteeseen eri kohteissa. Henkilöstön osalta olisi myös määritettävä tarvittavia rajoituksia verkon käytölle, jolloin varsinkaan avoimista langattomista verkoista ei työskenneltäisi verkkokaupan parissa.

Verkkokaupan asiakkaat sen sijaan voivat tulla ostoksille verkkokauppaan mistä verkosta tahansa. Tällöin on luotettava siihen, että verkkokaupan tietoliikenteen salaus on muilta osin riittävä ja annettava asiaankuuluva ohjeistus käyttäjälle, varsinkin omien käyttäjätunnustensa ja henkilötietojensa käsittelyyn. Asiakkaita on mahdollista myös ohjeistaa verkkokaupassa tarkemmin turvallisen yhteyden luomisessa. Seuraavaksi tarkastellaan käyttäjiä ja heille suunnattuja ohjeistuksia tarkemmin.

4.4 Käyttäjät

Käyttäjien kohdalla tietoturvan testaaminen ei ole täysin yksiselitteistä, sillä yksittäisen käyttäjän toiminta on käytännössä ennalta-arvaamatonta ja käyttäjät toimivat eri tavoilla toisiinsa nähden. Tämä on yksi suurista riskitekijöistä verkkokaupan tietoturvassa ja siitä huolimatta se jää usein tietoturvan testauksessa matalalle prioriteetille, jos siitä ei osata tunnistaa testattavia osa-alueita tai käyttäjien hallinta koetaan monimutkaisena.

Käyttäjiin kohdistuvan tietoturvatestauksen voikin nähdä enemmän ohjeistamiseen ja rajoituksiin keskittyvänä testaamisena, jolloin käyttäjää juurikin ohjataan toimimaan tietyllä tavalla ja rajoitetaan tarpeetonta toimintaa. Käyttäjän ohjeistamista voi testata käymällä verkkokaupasta läpi käyttäjän mahdolliset polut ja selvittämällä vastaako annetun opastuksen taso vaatimuksia. Toisaalta dokumentoidun ohjeistuksen toimivuuden voi selvittää vertaamalla sitä alussa laadittuun vaatimusmäärittelyyn ja testaamalla se käytännössä verkkokaupan toteutuksella. Edellisessä luvussa esitellyt käyttäjien rajoittamistoimet voidaan testata antamalla syötekenttiin vääränlaisia syötteitä ja IP-osoiterajoituksen kohdalla pelkästään käyttämällä ulkopuolista IP-osoitetta.

Verkkokaupan toimintojen ulkopuolelta käyttäjiin kohdistuvan manipuloinnin testaaminen voi kuulua omana osanaan testausprosessiin. Tällöin käyttäjiin voidaan kohdistaa manipulointiyrityksiä verkkokaupan ollessa jo toiminnassa ja tarkkailla käyttäjien reakti-

oita ja toimintaa ylipäänsä näissä tilanteissa. Jokainen oikea manipulointitilanne on kuitenkin yksilöllinen ja vihamieliset toimijat keksivät jatkuvasti uusia toimivampia tapoja manipuloida käyttäjiä, joten näiden manipulointiyritysten testaamista ei käytännössä saa kovinkaan kattavaksi. Käyttäjien riittävällä ohjeistuksella ja testaamisen aiheuttamalla tilanteeseen heräämisellä voi kuitenkin olla positiivisia vaikutuksia yksittäisten käyttäjien varovaisuudessa mahdollisia manipulointiyrityksiä vastaan. Testausta tärkeämpänä tässä asiassa voi olla jatkuva valvonta ja sopivan helpot epäiltyjen tapausten ilmiantamiskäytännöt.

Henkilöstön kouluttaminen on pitkällä tähtäimellä olennainen asia verkkokaupan turvallisuuden kannalta. Tätä varten laaditut koulutussuunnitelmat on hyvä tarkastaa testausvaiheessa, jotta ne varmasti sisältävät tietoturvaan liittyvät olennaisimmat kohdat käyttäjän ymmärtämällä tavalla ja ylipäänsä vastaavat alkuvaiheessa tehtyä vaatimusmäärittelyä.

4.5 Tarvittavat korjaukset

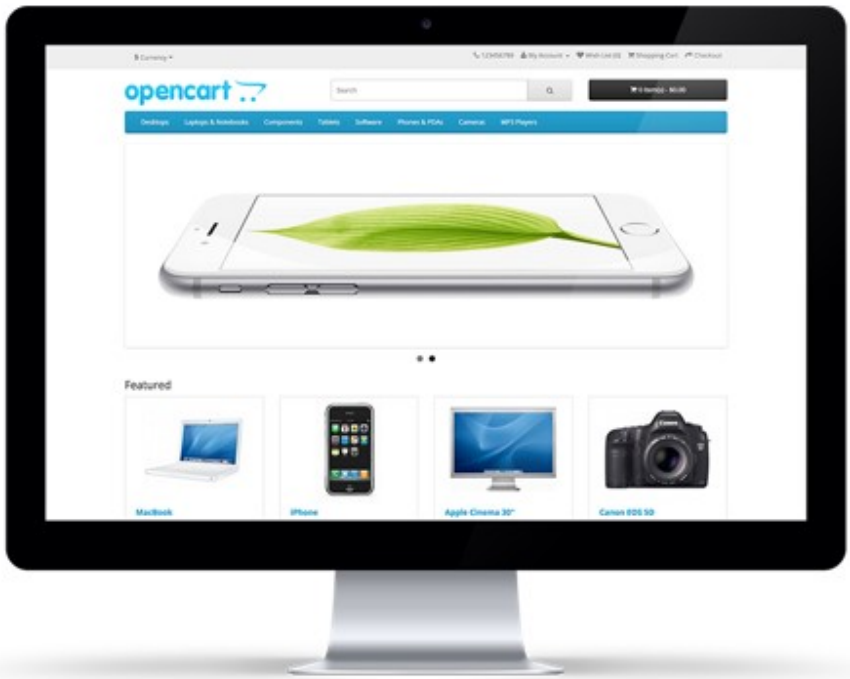
Tietoturvatestaamisen tavoitteena on todeta testattavan verkkokaupan täyttävän sille asetetut tietoturvavaatimukset, joten se ei siis missään tilanteessa voi kattaa kaikkia mahdollisia tietoturvauhkia, eikä näin ollen täysin suojattua verkkokauppaa ole mahdollista rakentaa. Testauksessa pyritään kuitenkin toteamaan olennaisimpien tietoturvauhkien olevan hallinnassa. Tietoturvan testaaminen tehdään käytännössä niin yksiselitteisellä tavalla, että verkkokauppa kestää siihen kohdistuvat testimielessä tehdyt rajutkin hyökkäysyritykset ja toisaalta on pystyttävä selkeästi toteamaan vaatimuksenmukaisia asioita verkkokaupan toteutuksesta ilman näitä testimielessä tehtyjä hyökkäyksiä.

Tietoturvatestaamisen pohjalta yritetään verkkokaupasta löytää asioita, jotka eivät täytä vaatimusmäärittelyn asettamia ehtoja tai tuota haluttua lopputulosta ja jotka näin ollen täytyy vielä korjata. Koko testausvaihetta voidaan pitää onnistuneena, jos testauksen aikana tietoturvasta on havaittu jotain korjattavaa. Tällöin nähdään, ettei testitapauksia ole luotu pelkästään olemassa olevan verkkokaupan suunnitelmien ja määrittelyn pohjalta, vaan siinä on otettu huomioon tietoturvaan yleisesti liittyviä uhkia.

Toisaalta määrittelyn ja suunnitelmien kuuluu olla sillä tasolla, ettei niiden pohjalta löydy perustavanlaatuisia tietoturvauhkia, kuten esimerkiksi vanhentuneet ohjelmistovalinnat. Testausvaiheessa testin suorittava taho voi myös havaita muita vaatimusmäärittelyyn kuulumattomia asioita, jotka on syytä korjata, ja nämä käsitellään tapauskohtaisesti niiden aiheuttaman uhan perusteella.

Nämä kaikki havaittavat korjaustarpeet sisältyvät vielä testausvaiheeseen, sillä korjaamisen jälkeen nekin tulee vielä testata uudelleen, eikä testausvaihetta voida sulkea ainakaan ennen kriittisten testitapausten hyväksyttyä testitulosta. Korjaukset palaavat siis testaajilta kommentteineen verkkokaupan toteuttajille, jotka tekevät tarvittavat korjaukset ja palauttavat korjatun version takaisin testaukseen.

Kun kaikki korjaukset tehty ja ne on testattu uudelleen hyväksytysti, sekä kaikki testitapaukset on saatu tämä pohjalta suljettua, on verkkokauppa valmiina käyttöön. Tällöin vastuu siirtyy testaavalta taholta ylläpitävälle taholle, joka aloittaa verkkokaupan jatkuvan seurannan ja hoitaa tulevien päivitysten tekemistä. Tässä vaiheessa verkkokauppa avataan lopulta asiakkaille, jolloin verkkokauppa alkaa tuottamaan. Alla oleva Kuva 6 esittää valmista verkkokauppaa asiakkaan näkökulmasta, jossa tuotteet on esitelty asiakasta houkuttelevalla tavalla [13].



Kuva 6. *Valmiin OpenCart-verkkokaupan asiakasnäkymä [13].*

Kuvan 6 esittämä verkkokaupan asiakasnäkymä on tietokoneen näytöltä, mutta verkkokaupan ulkoasu ja tyyli saattavat muuttua mobiililaitteissa erinäköisiksi riippuen erilai-

sista laitteen ominaisuuksista, kuten näytön koosta. Erilaisissa laitteissa saatetaan näyttää erilaisia sisältöelementtejä, kuten näytön kokoon perustuvia kuvien versioita, jolloin nämä kaikki eri versiot täytyy sisällyttää testaukseen.

5. TIETOTURVAN SEURANTA JA YLLÄPITO

Aiemmissa luvuissa todetun mukaisesti, verkkokaupan tietoturva ole täysin kunnossa tai pysy yllä kertaluontoisilla verkkokaupan toteuttamisen yhteydessä tehdyillä toimenpiteillä, vaan vaatii jatkuvaa seurantaa ja ylläpitoa. Tämä seuranta tarkoittaa käytännössä verkkokaupan toiminnan seuraamista monitoroimalla verkkokaupan tietoliikennettä, asiakkaiden toimia ja yleensä verkkokaupan toimintaa epätavallisten tapahtumien havaitsemiseksi. Seurannan on kuitenkin tapahduttava lain sallimissa puitteissa.

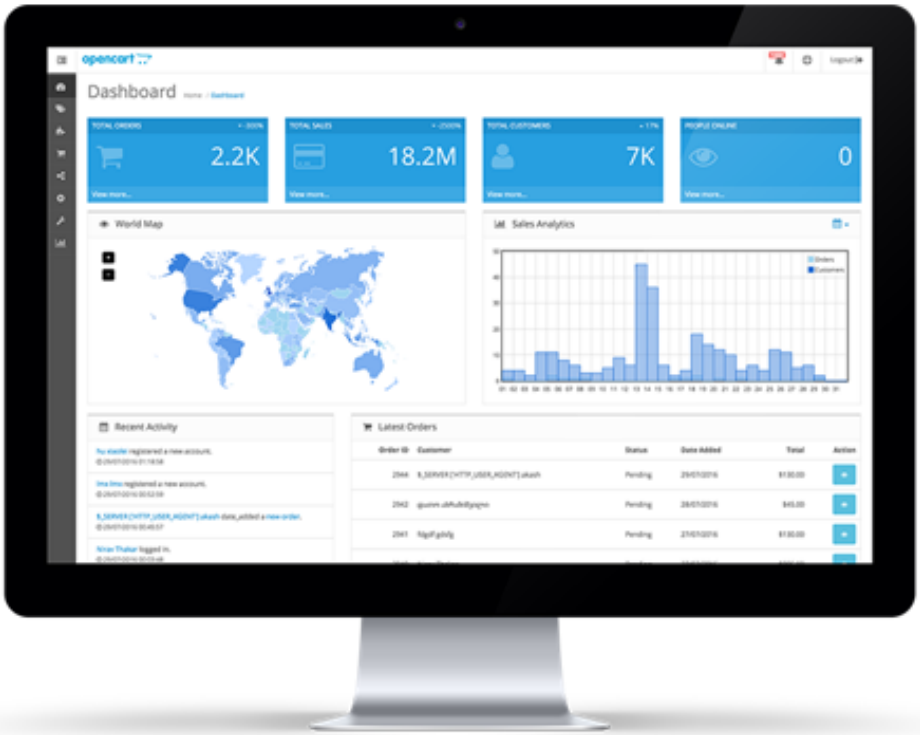
Verkkokaupan ylläpito puolestaan sisältää näiden epätavallisten tapahtumien ehkäisyä korjaavilla toimilla, sekä ohjelmisto- ja laitepäivitysten, kuten myös sisällöllisten asioiden hoitamista säännöllisellä tavalla. Nämä toimenpiteet saattavat aiheuttaa erilaisia lisätöitä verkkokaupassa aina alkuperäisen verkkokaupan muutostöistä testaamiseen. Verkkokaupan ylläpidon on myös peilattava tulevaisuuteen siinä määrin, että oikeat ja turvalliset ratkaisut osataan tehdä oikeassa aikataulussa.

5.1 Verkkokaupan seuranta

Verkkokaupat herättävät lähes poikkeuksetta mielenkiintoa vihamielisissä toimijoissa ja näin ollen verkkokaupat joutuvat jossain määrin erilaisten epäilyttävien toimien kohteiksi. Kuten aiemmin todettiin, verkkokaupan sisältämät tiedot ovat monessa merkityksessä arvokkaita. Vihamielisen toimijan hallussa arvokkainta tietoa on tiettävästi arkaluontoiset asiakastiedot, mutta myös maksulliset ladattavat kohteet ja verkkokaupan kautta selvitettävissä olevat yritykseen kohdistuvat salaiset tiedot, kuten julkaisemattomat uudet tuotteet ja niiden ominaisuudet.

Verkkokaupan maineen ja tulevaisuuden kannalta on tärkeää saada pidettyä kaikki salattava tieto turvassa. Tämän vuoksi seuranta on verkkokaupan kannalta hyödyllinen tapa, jonka avulla nähdään mitä verkkokaupassa käytännössä tapahtuu.

Verkkokauppaohjelmistossa ja varsinkin sen hallintapaneelissa voidaan seurata verkkokaupan toimintaan liittyviä asioita. Näistä luonnollisena seurantakohteena on verkkokaupan tilaustiedot, joissa normaaleista poikkeavat tai keskeytyneet tilaukset voivat olla merkkejä vihamielisestä toiminnasta. Näitä merkkejä voivat myös olla lomakkeiden ja kenttien syötteisiin tulevat epämääräiset kokeilut, sekä tietokannasta löytyvät poikkeamat. Verkkokaupassa ja sen hallinnassa ilmestyvät virheilmoitukset voivat omalta osaltaan ennakoida mahdollista hyökkäystä kauppaa kohtaan. Kuva 7 alla esittää verkkokaupan hallintapaneelin tilastoja verkkokaupan käytöstä.



Kuva 7. *OpenCart-verkkokauppaohjelmiston hallintapaneelin tilastosivu [13].*

Vihamielinen toiminta ei kuitenkaan välttämättä tapahdu suoraan verkkokauppaohjelmiston kautta, vaan voi hyödyntää muita aiemmissa luvuissa mainittuja kanavia, kuten tietoliikenneverkkoja ja käyttäjiä. Tietoliikenneverkon seuranta on monessa mielessä haastavaa, sillä tietosuojan ja lakien vuoksi tässä tapauksessa voidaan tehdä vain rajattuja seurantatoimenpiteitä. Verkkokaupan tietoliikenteestä voidaan havainnoida kuitenkin paljon liikennettä aiheuttavia tahoja varsinkin pääsääntöisen myyntialueen ulkopuolelta tulevaan tietoliikenteeseen. Toisaalta seuranta voi kohdistua myös poikkeavan laatuiseen tietoliikenteeseen, joka ei suoranaisesti liity verkkokaupan tavanomaiseen toimintaan.

Verkkokaupan palvelimella tapahtuva seuranta rajoittuu myös tietosuojasta johtuen teknisiin yksityiskohtiin, kuten käyttäjäoikeuksista riippuen prosesseihin ja kuormitukseen. Palvelimella olevat tiedostot ja kansiot, sekä niiden käyttöoikeudet, eli chmod-arvot voivat muuttua vihamielisen toiminnan johdosta, jolloin niiden seuraaminen voi johtaa epäilyttävän toiminnan jäljille.

Käyttäjien osalta seurantaa voidaan suorittaa käyttämällä lokitiedostoja sellaisista verkkokaupan alueista, johon pääsyä pyritään rajaamaan. Näin toimimalla voidaan selvittää

tietoja käyttäjien toiminnasta. Käyttäjillä tarkoitetaan tässä tapauksessa pääsääntöisesti verkkokaupan henkilöstöä, jolloin voidaan saada viitteitä siitä, onko käyttäjän tunnukset esimerkiksi kaapattu.

Verkkokaupan tietoturvan seurantaa voidaan toteuttaa myös erilaisilla ulkoisilla työkaluilla, kuten yleensä verkkosivuja tutkivilla skannereilla. Nämä skannerit etsivät verkkosivuista ohjelmointivirheitä ja versioihin liittyviä heikkouksia, mutta tutkivat myös mahdollisia palvelimella havaittuja puutteita. Toisin sanoen skannerit etsivät ylläpidon avuksi verkkosivujen haavoittuvuuksia, joita hakkerit voisivat hyödyntää. Tällainen skanneri on esimerkiksi ilmainen ScanMyServer -palvelu, jonka kautta saa raportin verkkosivuston jokaisen sivun haavoittuvuudesta valinnan mukaan joko viikoittain tai kuukausittain. Jos verkkosivut täyttävät riittävän tietoturvatason, palvelu antaa käyttöön sertifikaattikuvakkeen näytettäväksi verkkosivuilla aina seuraavaan skannaukseen asti. Tämä sertifikaattikuvake voi lisätä verkkokaupassa vierailevan asiakkaan luottamusta verkkokauppaa kohtaan. [18]

Verkkokaupan tietoturvaa voi seurata myös palvelimella olevien tiedostojen ja kansioiden säännöllisellä virustarkistuksella palvelimelle erikseen asennettavissa olevalla virustarkastusohjelmalla. Tällaisesta virustarkastusohjelmasta on hyvänä esimerkkinä Cisco Systems -nimisen yrityksen kehittämä avoimen lähdekoodin ClamAV Virus Scanner -ohjelma, jonka avulla virustarkistus onnistuu palvelimella sijaitsevien verkkokaupan tiedostojen ja kansioiden lisäksi esimerkiksi koko verkkokaupan sähköpostikansiossa. Ohjelman avulla saadaan siis seurattua tiedostojen ja kansioiden seasta palvelimelle mahdollisesti ilmestyvää haitallista sisältöä, sekä voidaan kontrolloida sitä. [2]

Erilaisten skannerien ja virustorjuntojen lisäksi on olemassa monenlaisia muita työkaluja verkkosivujen seurantaan, sekä manuaalisesti että automaattisesti, mutta tämä diplomityö ei ota sen tarkemmin kantaa kaikkiin saatavilla oleviin erilaisiin työkaluihin.

5.2 Verkkokaupan ylläpito

Sopivan tietoturvatason säilyttämiseksi verkkokauppaa on ylläpidettävä säännöllisesti. Päivityksistä huolehtiminen on ylläpidon perusasioita ja varsinkin kriittiset tietoturvapäivitykset on syytä tehdä viipymättä. Päivittäminen voi kuitenkin olla hidas prosessi, varsinkin verkkokauppaohjelmiston tapauksessa, jos verkkokaupassa on paljon varsinaiseen ohjelmistoon tehtyjä muokkauksia tai lisäosia. Tällöin päivittäminen vaatii selkeää suunnitelmaa ja yhteistyötä eri tahojen välillä, sillä verkkokaupan toiminta on varmistettava testaamalla muutosten vaikutusta. Vaikka testaaminen voidaan suorittaa omassa erillisessä ympäristössään, voidaan verkkokauppa silti joutua ajamaan hetkellisesti alas

päivityksen ajaksi. Tällöin asiakkaat eivät pääse tekemään ostoksia ja verkkokaupan tulot pysähtyvät, joten tämän ajan minimointi on verkkokaupan intresseissä.

Verkkokaupan päivitys tapahtuu yleensä tietyissä sykleissä verkkokauppaohjelmiston tai siihen liittyvien lisäosien ja palvelinohjelmistojen julkaisuaikataulujen mukaan. Monesti nämä kaikki eri päivitykset pyritään tekemään samalla kertaa, jolloin päivityskertojen määrää saadaan vähennettyä ja ylläpidollisia resursseja säästettyä. Tällöin verkkokaupan palvelimella olevaan testiympäristöön tehdään kaikki valitut päivitykset ja mahdolliset niistä johtuvat korjaus- tai muutostyöt. Päivitykset yleensä muuttavat jotain toimintaa verkkokaupassa niin, että se aiheuttaa varsinkin kustomoiduissa verkkokaupoissa virhetilanteita tai päivitysten laatu ei esimerkiksi kaikkien lisäosien kohdalla ole kovin korkealla tasolla, jolloin verkkokauppaan päivitysten johdosta tehtävät korjaus- ja muutostyöt voivat viedä paljon aikaa ja muita resursseja.

Päivitystyön jälkeen verkkokaupan toiminta testataan vielä erillisessä testausvaiheessa aiemmassa luvussa esitellyn testausprosessin mukaisesti. Tässä testausvaiheessa ei välttämättä testata koko verkkokauppaa, vaan testaukset voidaan kohdistaa niille toiminnallisuuksille, joihin päivitykset vaikuttavat. Kun testaus on hyväksytysti suoritettu, voidaan uusi päivitetty versio siirtää testiympäristöstä varsinaiseen tuotantoympäristöön, jossa asiakkaille näkyvä verkkokauppa sijaitsee.

Verkkokauppaohjelmiston lisäksi laitteet ja niiden ohjelmistot vaativat ajoittain päivityksiä. Näitä ovat lähinnä verkkokaupan palvelimen ja henkilökunnan laitteiston päivitykset. Fyysinen palvelin säilyttää verkkokauppakäytössä yleensä tehokkuutensa pitkään, mutta sen ohjelmistoversiot vaativat ajoittaista päivittämistä ja palvelimelle voidaan joutua myös asentamaan uusia ohjelmistoja verkkokaupan kehittyessä. Tässä diplomityössä ei oteta tarkemmin kantaa laitteiden tai niiden ohjelmistojen päivityksiin aiemmin mainitun palvelimen ohjelmistojen päivityksen lisäksi.

Päivittämisen jälkeen seuraa uusien tulevien päivitysten ajoittaminen, jonka tekeminen pohjaa ohjelmistojen päivitysaikatauluihin ja sisältöihin. Tämä tieto päivityksistä ei ole aina saatavilla kovinkaan pitkällä varoitusajalla, mutta käytännössä useilla eri ohjelmistoilla on tietoturvapäivityksille säännölliset julkaisuaikataulut. Alla oleva Taulukko 5 kuvaa OpenCart-verkkokauppaohjelmiston päivitysaikataulua kymmenen viimeisimmän päivityksen osalta [15].

Taulukko 5. *OpenCart-verkkokauppaohjelmiston päivitysaikataulu kymmenen viimeisimmän päivityksen osalta [15].*

Ohjelmistoversio	Julkaisupäivämäärä
3.0.3.6	July 20, 2020
3.0.3.5	July 18, 2020
3.0.3.3	May 1, 2020
3.0.3.2	April 9, 2019
3.0.3.1	January 7, 2019
3.0.3.0	January 2, 2019
3.1.0.0_b	July 27, 2017
3.0.2.0	July 18, 2017
3.0.1.2	July 7, 2017
3.0.1.1	July 4, 2017

Taulukosta 5 havaitaan kyseisen verkkokauppaohjelmiston päivitysten ajallisen satunnaisuuden, joka vaikeuttaa tulevien ylläpitotoimien suunnittelua. Samalla havaintaan myös uusien ohjelmistopäivitysten ilmestymisen nopea tahti ohjelmistoversion alkuvaiheessa.

Verkkokaupan ylläpitoon kuuluu päivittämisen lisäksi myös muita toimenpiteitä, kuten pienten korjausten tekeminen ja kaupan toimivuudesta huolehtiminen.

5.3 Tulevaisuuden visiot

Verkkokaupan ylläpidon kannalta tulevaisuuden ratkaisut ja teknologiat vaikuttavat nykyisen verkkokaupan elinkaareen ja uuden rakennusprojektin aloitukseen. Teknologialtaan tulevaisuudessa vanhaksi määriteltävä nykyinen verkkokauppa on todennäköisesti korvattava uudella asennuksella, kun tämä vanha verkkokauppa todetaan sopimattomaksi sen ajan tarpeisiin tai sen elinkaari päättyy esimerkiksi päivitysten loppumisen myötä.

ICT-alalla on ollut välillä vaikea ennustaa tulevaisuutta alan luonteesta johtuen, sillä kaikkia uusia keksintöjä on mahdotonta spekuloida etukäteen. Joitain suuria linjoja on kuitenkin aiemminkin osattu ennustaa ja ehkä juuri menneeseen katsominen, sekä nykyisen kehityksen seuraaminen, voivat auttaa jossain määrin luomaan visioita verkkokaupan tulevaisuudesta.

Verkkokaupan osalta yhtenä suurena avoimena kysymyksenä voidaan pitää sitä, mitä verkko tulevaisuudessa tarkoittaa. Erinäiset tahot ovat suunnitelleet tai rakentaneet omia verkkojaan ja tämän trendin jatkuessa ne saattavat muodostaa ainakin teknisesti ja alueellisesti rajattuja omia kokonaisuuksiaan, kun nykyisin verkoksi käsitetään yleisesti maailmanlaajuinen Internet.

Varsinkin Venäjän toimet oman sisäisen verkon rakentamisessa ovat olleet näkyvästi julkisuudessa. Vaikka Venäjä on vasta kokeillut eristäytymistä muun maailman verkosta samalla teknologialla, voi se olla yksi askel siihen suuntaan, että maailmaan tulee jatkossa useampia teknologisesti toisistaan erilaisia ja maantieteellisesti rajattuja verkkoja. [4]

Verkkokaupan kannalta usean rinnakkaisen verkon kehitys voi tarkoittaa markkina-alueen rajautumista tai usean verkkokaupan pystyttämistä eri verkkoihin. Toisaalta myös verkkokaupan tekninen toteutus voi kokea muutoksia, jos mahdollisten alueellisten verkkojen toimintamallit poikkeavat suuresti toisistaan.

Toisaalta yksi suuri kysymys verkkokaupan tulevaisuudessa voi myös olla pienten yksittäisten verkkokauppojen katoaminen ja myynnin keskittyminen suuriin palveluihin. Tämä ilmiö on vahvistunut varsinkin Yhdysvalloissa, jossa verkkokaupan jättiläinen Amazon on vallannut paikallisen verkkokaupan markkinaosuudesta jo noin puolet. [25]

Kun ostajat siirtyvät hakemaan tuotteita suurista yksittäisistä verkkokaupoista, jää pienille toimijoille entistä vähemmän asiakkaita. Tässä tilanteessa pienet verkkokaupat ajautuvat helposti käyttämään suuren toimijan alustaa ja hylkäävät oman verkkokauppansa. Yksi mahdollinen skenaario tulevaisuudella onkin siis, että verkkokauppojen määrä voi merkittävässä määrin vähentyä ja verkkokaupan itsenäinen pyörittäminen ei ole enää kannattavaa.

Kolmantena suurena kysymyksenä voi tulevaisuuden osalta ajatella myös laitteiden ja sitä myötä teknologian kehittymistä, joka jollain tavalla ajaa muutoksia verkkokaupan teknologisiin ratkaisuihin tai tekee verkkokaupasta tarpeettoman kaupankäynnin muodon, jos tuotteet päätyisivät asiakkaille jonkinlaisen älykotiin ja älytoimistoon liittyvän ratkaisun kautta.

Mikään kehityskulku ei välttämättä kuitenkaan tuo äkillistä muutosta verkkokauppaan, vaan luultavasti trendit tulevat ajamaan vähitellen verkon kaupankäyntiä tiettyyn suuntaan. Tässä menestyvän verkkokaupan onkin pystyttävä seuraamaan kehitystä ja pystyttävä tekemään oikeanlaisia linjauksia tulevaisuuden varalle.

Myös big datan, data-analytiikan ja koneoppimisen kehittyminen voi vaikuttaa merkittävästi jatkossa verkkokaupan kehittymiseen ja käytettyihin ratkaisuihin, yksinkertaistamalla verkkokaupan toimintaa asiakkaan näkökulmasta ja mahdollisesti myös poistamalla nykyisen verkkokaupan mallin integroitumalla vahvemmin toisiin tulevaisuuden kanaviin. Tämä diplomityö ei ota kuitenkaan sen tarkemmin kantaa muihin mahdollisiin tulevaisuuden näkymiin.

6. YHTEENVETO

Tässä diplomityössä käsiteltiin verkkokaupan tietoturvaa yleisesti keskittymättä tiettyyn verkkokauppaohjelmistoon, painopisteen ollessa ilmaisissa avoimen lähdekoodin verkkokauppaohjelmistoissa. Käsittelyyn sisältyi tietoturvaan yleisesti liittyviä asioita, kuten ohjelmistoja, laitteistoja ja tietoverkkoja. Näiden lisäksi tarkasteltiin myös käyttäjien roolia eri tilanteissa. Diplomityössä tuotiin esille myös ohjelmistoprojektin puolelta yleisesti ohjelmistoprojektin vaiheita ja tarkasteltiin niitä verkkokaupan tietoturvan näkökulmasta. Myös olennaiset yleisesti verkkosivuihin ja tietojenkäsittelyyn liittyvät asiat, metodit ja työkalut esiteltiin pintapuolisesti.

Diplomityön varsinainen sisältö alkoi johdannolla, joka on ensimmäinen luku. Siinä esiteltiin pääpiirteissään mitä diplomityössä käsitellään ja avattiin työn rakennetta luku kerrallaan.

Johdannon jälkeisessä toisessa luvussa esiteltiin aluksi teoriaa siitä, minkälaisia asioita verkkokaupan tietoturvan osalta on otettava huomioon ja miten verkkokaupasta kiinnostuneet vihamieliset toimijat yleensä hyödyntävät omia keinojaan. Tämä toinen luku käsitteli teoriaa verkkokauppaohjelmistojen, palvelinten, päätelaitteiden ja niiden ohjelmistojen, sekä tietoliikenneverkkojen ja käyttäjän näkökulmasta.

Kolmannessa luvussa käsiteltiin turvallisen verkkokaupan rakentamista toisen luvun teorian pohjalta. Luvun alussa esiteltiin vielä yleisimpiä tietoturvauhkia ja niiden vaikutusta verkkokaupan rakentamiseen. Seuraavaksi käytiin läpi ohjelmistoprojektien erilaiset vaiheet vesiputousmallia hyödyntämällä ja käsiteltiin vaatimusmäärittelyä tarkemmalla tasolla. Tämän jälkeen perehdyttiin laitteiden ja ohjelmistojen valintaan vaatimusmäärittelyn pohjalta, jota seurasi valittujen ohjelmistojen asennus ja konfigurointi. Verkkokaupan rakentamisen jälkeen käytiin yleisellä tasolla läpi verkkokaupan testaaminen tietoturvan näkökulmasta. Lopuksi tarkasteltiin käyttäjien ohjeistamista ja ohjaamista erilaisin keinoin.

Neljäs luku keskittyi verkkokaupassa ohjelmistoprojektin testausvaiheeseen ja testauksessa löydettyjen korjattavien asioiden käsittelemiseen. Alussa esiteltiin testaamista ja siihen liittyviä käytäntöjä yleisellä tasolla. Seuraavaksi käsiteltiin verkkokauppaan liittyvien ohjelmistojen, laitteiden ja verkkojen testaamista. Lopuksi tarkasteltiin testausta käyttäjien näkökulmasta ja perehdyttiin testauksessa löydettyjen ongelmakohtien korjaukseen.

Viidennessä luvussa käsiteltiin verkkokaupan seurantaa ja ylläpitoa. Tämä pohjautui edellisen luvun testattuun valmiiseen verkkokauppaan, johon asiakkaat tulevat ostoksille. Ensimmäisenä käsiteltiin seurantaan liittyviä mahdollisuuksia ja nostettiin esille sallitut keinot verkkokaupan tietoturvan seurantaan. Seuraavaksi perehdyttiin verkkokaupan ylläpitämiseen, eli käytännössä siihen, miten verkkokauppa pidetään jatkossakin turvallisena asiakkaalle ja verkkokaupalle itselleen. Viimeisessä kohdassa pohdittiin havaittujen trendien pohjalta verkkokaupan tulevaisuuden näkymiä kolmen keskeisen linjavedon perusteella.

Lopuksi tämä kuudes luku vetää yhteen diplomityön sisällön ja oleelliset asiat tiiviissä muodossa. Tämän diplomityön pohjalta nähdään, että verkkokaupan tietoturvaa on käytännössä mahdotonta saada täysin aukottomaksi. Tämä johtuu siitä, että verkkokauppaan, kuten yleensä muihinkin verkkosivustoihin, kytkeytyy niin monta tekijää, ettei kaikkien täydellinen hallitseminen ja suojaaminen ole mahdollista tai ylipäätään järkevää projektirajoitusten puitteissa. Siksi onkin tärkeää ymmärtää mitkä asiat ovat olennaisimpia ja kuinka verkkokaupan jatkuva kehitys toimii.

Verkkokaupan tietoturvaan kuuluu jokaisesta ohjelmistoprojektin vaiheesta erilaisia olennaisia tekijöitä. Suunnittelu ja määrittely on tärkeää verkkokaupan alkuperäisen version suojaamiseksi, vaikka siinä suunnitelmat tehdään pitkällä tähtäimellä, eli otetaan huomioon myös verkkokaupan päivitettävyys. Näihin kuuluvat ohjelmistojen valinnat ja muut ratkaisut.

Toteutus- ja testausvaiheet sisältävät olennaiset ratkaisut verkkokaupan pystyttämiseen ja toteutuksen toimivuuden toteamiseen. Näissä vaiheissa valittu kokoonpano rakennetaan toimivaksi verkkokaupaksi ja sen olennaiset ominaisuudet testataan tietoturvan näkökulmasta. Ajatuksena on saada kokonaisuudesta mahdollisimman käytettävä, mutta myös turvallinen, jotta arkaluontoiset tiedot eivät päätyisi verkkokaupasta vääriin käsiin vihamieliselle toimijalle.

Ylläpitovaiheessa keskitytään olemassa olevan verkkokaupan pitämiseen toimintakuntoisena ja turvallisena. Tämä hoidetaan käytännössä seurannalla ja korjauksilla, sekä päivityksillä. Verkkokauppa pysyy turvallisena niin pitkään, kuin sen tietoja ei ole päässyt vuotamaan ulkopuolisille. Seuranta, korjaukset ja päivitykset pyrkivät estämään tietojen vuotamisen ja niitä on tehtävä jatkuvalla periaatteella teknologian ja hyökkäystaktiikoiden kehittymisen mukaan, sekä uusien haavoittuvuuksien löytyessä.

Verkkokaupan tulevaisuus riippuu vahvasti siitä, mitkä trendit tulevat jatkossa vaikuttamaan eniten. Tässä diplomityössä on tarkasteltu tulevaisuutta kolmesta eri näkökulmasta, verkkojen jakautumisen, verkkokaupan keskittymisen ja teknologisen kehityksen

kautta. Nämä kaikki ovat diplomityön tekijän omia näkemyksiä alan kehityksestä uutisoinnin ja tulevaisuudenkuvan pohjalta.

Diplomityön pohjalta voidaan ajatella jatkotutkimusta nykyisen diplomityössä käsitellyn verkkokaupan ja sen teknologioiden kehityksestä, mutta myös yleisesti ajateltuna verkkokaupan tulevaisuuden ja sen mahdollisten kehityssuuntien vaikutusta nykymuotoiseen verkkokauppaan.

Ensimmäisen vaihtoehdon tapauksessa jatkotutkimus voi keskittyä tarkemmalla tasolla erilaisiin suojausmenetelmiin, joissa avataan teknisiä yksityiskohtia tai tutkitaan yksittäisiä tietoturvaan liittyviä työkaluja. Toisaalta käsittelyä voi laajentaa myös keskittymällä tiettyyn verkkokauppaohjelmistoon tai vertailemalla erilaisia verkkokauppaohjelmistoja keskenään.

Toinen vaihtoehto olisi huomattavasti teoreettisempi ja spekulatiivisempi, sillä siinä pystytään hyödyntämään tämänhetkisiä veikkauksia tulevaisuuden linjoista ja tarkkailla trendejä, joista saa riittävästi tietoa lähdemateriaaleiksi. Tulevaisuuden osalta olisi kuitenkin esitettävä näiden trendien tai veikkauksien pohjalta erilaisia kehitysmalleja tai fokusoitava tulevaisuuden arvaaminen yhden vahvimmalta näyttävän pohjan varaan.

Näiden ajatusten pohjalta voi todeta, että diplomityöstä voisi tehdä vielä paljon eri suuntiin lähtevää jatkotutkimusta joko väitöskirjan tai toisen diplomityön tasolla.

LÄHTEET

[1] Browser Market Share Worldwide June 2019 - June 2020, Statcounter, 2020. Saatavissa: https://gs.statcounter.com/browser-market-share

[2] ClamAV Virus Scanner, Cisco Systems, 2020. Saatavissa: https://www.clamav.net/

[3] B. Drouin, kuva, 2020. Saatavissa: https://pixabay.com/fi/photos/verkko-palvelin-järjestelmän-2402637/

[4] T. De Fresnes ja S. Brännare, Venäjä kokeili netin sulkemista muulta maailmalta – asiantuntijat: Kyse on informaatiotilan hallinnasta ja sotilaallisesta pelotteesta, Yle Uutiset 2019. Saatavissa: https://yle.fi/uutiset/3-11134570

[5] P. Gralla, Your Windows PC may become collateral damage in any conflict with Iran, ComputerWorld, 2020. Saatavissa: https://www.computerworld.com/article/3513358/your-windows-pc-may-become-collateral-damage-in-any-conflict-with-iran.html

[6] V-P. Hämäläinen ja S. Tuominen, Joku julkaisi 16 000 suomalaisen henkilötunnukset netissä kuusi vuotta sitten – nyt niillä tehtaillaan tuhansia rikoksia vuodessa, Yle Uutiset, 2017. Saatavissa: https://yle.fi/uutiset/3-9914817

[7] Increment Security, 7. julkaisu, Stripe, 2018

[8] Installation, OpenCart, 2020. Saatavissa: http://docs.opencart.com/en-gb/installation/

[9] A. Karkimo, Verkon suurin maalitaulu? – Nollapäivähyökkäykset taas kiivaasti käynnissä, Tivi, 2020, Saatavissa: https://www.tivi.fi/uutiset/verkon-suurin-maalitaulu-nollapaivahyokkaykset-taas-kiivaasti-kaynnissa/f232b2a3-ef12-46af-bf94-2ef700fb963c

[10] K. Leswing, A password for the Hawaii emergency agency was hiding in a public photo, written on a Post-it note, Business Insider, 2018. Saatavissa: https://www.businessinsider.com/hawaii-emergency-agency-password-discovered-in-photo-sparks-security-criticism-2018-1?r=US&IR=T

[11] Linux Users and Groups, Linode, 2020. Saatavissa: https://www.linode.com/docs/tools-reference/linux-users-and-groups/

[12] NSA:n kädenjälki myös Androidin ja Linuxin ytimessä, Digitoday, 2013. Saatavissa: https://www.is.fi/digitoday/tietoturva/art-2000001802180.html

[13] Opencart Demonstration, OpenCart, 2020. Saatavissa: https://www.opencart.com/index.php?route=cms/demo

[14] Operating System Market Share Worldwide June 2019 - June 2020, Statcounter, 2020. Saatavissa: https://gs.statcounter.com/os-market-share

[15] Previous & Release Notes, OpenCart, 2020. Saatavissa: https://www.opencart.com/index.php?route=cms/download/history

[16] N. Rastogi, OpenCart Security Issues – Top Attacks on OpenCart March 29 2020, Astra IT, 2020. Saatavissa: https://www.getastra.com/blog/cms/opencart-security/opencart-security-issues-top-attacks/

[17] E. Rescorla, The Transport Layer Security (TLS) Protocol Version 1.3, Internet Engineering Task Force, 2018. Saatavissa: https://tools.ietf.org/html/rfc8446

[18] ScanMyServer, Beyond Security, 2020. Saatavissa: https://scanmyserver.com/my_account/

[19] P. Tapala, Miljoonissa Android-laitteissa jo pitkään vakava tietoturva-aukko – korjaus MediaTek-piirillisille laitteille tulossa vasta nyt, mobiili.fi, 2020. Saatavissa: https://mobiili.fi/2020/03/03/miljoonissa-android-laitteissa-jo-pitkaan-vakava-tietoturva-aukko-korjaus-mediatek-piirillisille-laitteille-tulossa-vasta-nyt/

[20] Top Ten Web Application Security Risks, OWASP, 2020. Saatavissa: https://owasp.org/www-project-top-ten/

[21] M. Walker, CEH Certified Ethical Hacker Exam Guide, 3. painos, Mc Graw Hill, 2017.

[22] J. Warnimont, 20 Best Open Source and Free Ecommerce Platforms for 2020, Ecommerce platforms, 2020, Saatavissa: https://ecommerce-platforms.com/articles/open-source-ecommerce-platforms

[23] Q. Wong, TikTok accused of secretly gathering user data and sending it to China, CNET, 2019. Saatavissa: https://www.cnet.com/news/tiktok-accused-of-secretly-gathering-user-data-and-sending-it-to-china/

[24] Yleinen tietosuoja-asetus, Sinun Eurooppasi, Euroopan Unioni, 2020. Saatavissa: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm

[25] A. Ylä-Anttila, Vanhanaikaiset yritykset ovat vaarassa päätyä Amazonin orjiksi – ”Se, toimiiko Amazon fyysisesti Suomessa, ei ole olennaista”, Mikrobitti, 2019. Saatavissa: https://www.mikrobitti.fi/uutiset/vanhanaikaiset-yritykset-ovat-vaarassa-paatya-amazonin-orjiksi-se-toimiiko-amazon-fyysisesti-suomessa-ei-ole-olennaista/8a781938-87bd-403d-ae3b-2cee68f47328